



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI



New Zealand  
Security Intelligence  
Service  
Te Pā Whakamarumaru

## Joint Policy Statement: JPS - 013

### Making a Protected Disclosure

Policy Owner	Director Strategy, Governance and Performance, GCSB Deputy Director-General, NZSIS
Policy Administrator	Compliance and Policy Manager, GCSB Manager, Compliance and Risk, NZSIS
Approval Authority	Director-General, GCSB Director-General, NZSIS
Approval Date	27 July 2018
Review Date	Three years from signing

## Contents

Purpose.....	3
Background .....	3
Scope.....	3
Definitions .....	4
Process.....	5
<i>Who Can Make a Protected Disclosure?</i> .....	5
<i>What is a Protected Disclosure?</i> .....	5
<i>How a Protected Disclosure Should be Made</i> .....	6
<i>Who Disclosures May be Made to</i> .....	7
<i>Information to be Provided at Time of Disclosure</i> .....	7
<i>Obligations on Recipient of a Protected Disclosure</i> .....	8
<i>Response to a Disclosure</i> .....	9
<i>Conduct of Any Investigation</i> .....	9
<i>Decision and Response</i> .....	10
<i>Advice to Person Disclosing</i> .....	10
<i>When the Matter is Not a Serious Wrongdoing</i> .....	10
Protections for Persons Making a Disclosure .....	11
<i>Immunity From Civil or Criminal Proceeding Associated With Making a Disclosure</i> .....	11
<i>Confidentiality</i> .....	11
<i>Protection from Retaliation and Victimisation</i> .....	11
<i>Security Clearance</i> .....	12
Support for Person Making a Disclosure .....	12
Making a Disclosure Outside the GCSB or NZSIS .....	13
<i>Making a Disclosure to the Inspector-General</i> .....	13
<i>Making a Disclosure to a Minister Responsible for an Intelligence and Security Agency or the Prime Minister</i> .....	14
Further Information and Guidance .....	14
Previous Policy Revoked.....	15
Approval .....	16
Summary of Minor Amendments .....	17

## Purpose

1. New Zealand is held in high regard for the standards of honesty, openness, transparency and integrity in the State Services, but our reputation depends on our ability to build and maintain a culture that promotes speaking up about wrongdoing.
2. The purpose of this policy statement is to set out the internal procedures for GCSB and NZSIS staff to make a protected disclosure about a serious wrongdoing under the provisions of the Protected Disclosure Act 2000 (the Act). It also sets out the GCSB and NZSIS response to concerns raised by staff about the actions of the GCSB or NZSIS that are not assessed to be a protected disclosure.
3. People working for the NZSIS and GCSB can get information about this policy, the process of making a protected disclosure, and whether a disclosure may be a protected disclosure from:
  - a. The Chief Legal Advisor for GCSB or NZSIS;
  - b. The Managers of Compliance and Policy of GCSB and NZSIS;
  - c. The Chief People Officer for the GCSB and NZSIS; or
  - d. The Inspector-General.
4. This information can be provided on a confidential basis and may be obtained at any stage of the process.
5. Further information and guidance on making a protected disclosure can be found on the GCSB intranet, on the NZSIS intranet, on the Office of Inspector-General of Intelligence and Security's website [www.igis.govt.nz](http://www.igis.govt.nz), and on the States Services Commission website under their "Speaking Up" material [www.ssc.govt.nz/speaking-state-services](http://www.ssc.govt.nz/speaking-state-services).

## Background

6. The Act protects current and past employees and others who wish to make disclosures of serious wrongdoing in or by their organisations. People engaged by the intelligence and security agencies who make protected disclosures are protected from civil or criminal liability or sanction by their employer.

## Scope

7. These procedures apply to the making of a protected disclosure about serious wrongdoing (or a belief in good faith about serious wrongdoing) by the GCSB or the NZSIS at any time.
8. Protected disclosures may be made by any former or current GCSB/NZSIS employee, contractor, person seconded from another organisation to the GCSB/NZSISs6(a) person engaged to do work for the GCSB/NZSIS or any person who works for the GCSB or NZSIS as a volunteer.

- ██████████
9. There are a range of disclosures that can be made by current or former GCSB/NZSIS employees. This policy covers a specific type of disclosure as set out in paragraphs 12–16 below. This policy does not cover:
- a. disclosures made internally to GCSB/NZSIS that do not meet the protected disclosure criteria;
  - b. the management of concerns that are about the treatment of an employee by their manager or co-workers. Employment issues are dealt with in accordance with employment agreements, fixed term or other contracts, and human resources policies. Human Resource related documents can be found on the agency intranet in the HR Toolkit; and
  - c. GCSB/NZSIS employees or former employees making a complaint to the Inspector-General under section 171(3) of the ISA or disclosures to the Inspector-General under section 160 of the ISA. This is covered separately in advice from the Inspector-General.
10. This JPS does not cover unauthorised disclosures (for example; media leaks). In the case of an unauthorised disclosure GCSB/NZSIS security policies and procedures will apply.

## Definitions

**Act** means the Protected Disclosures Act 2000

**Appropriate authority** for the GCSB or NZSIS means **only** the Inspector-General. The Appropriate Authority may provide advice and guidance (section 6B) and a disclosure may be made to the appropriate authority in specified circumstances (section 9)

**Classified information**<sup>1</sup> means

- (a) information that-
  - (i) is, or was, official information; and
  - (ii) is classified under the New Zealand Government Security Classification System as being accessible only to persons who have a national security clearance;
- (b) foreign government information that is-
  - (i) classified in a foreign country; and
  - (ii) accessible only to persons having a government-sponsored national security clearance

**New Zealand Government Security Classification System** means the security classification system applying to official information that is published (and from time to time amended) on an Internet site maintained by or on behalf of the NZSIS. Note that this will include protectively marked information at confidential or above in accordance with the Protective Security Requirements (PSR)

---

<sup>1</sup> Definition taken from the Crimes Act 1961, section 78AA (3)

**Date of the disclosure** means the date the disclosure is made by the discloser verbally or in writing

**Discloser or person making a disclosure** means any person entitled to make a protected disclosure under the Protected Disclosures Act 2000

**Inspector-General** is the Inspector-General of Intelligence and Security

**Legal professional privilege** means communications or information shared between an individual and their legal advisor that is intended to be confidential and is in relation to obtaining or requesting legal services. Legal advice provided to the organisation by the NZSIS and GCSB Legal teams is protected by legal professional privilege

**Protection** means protection from civil or criminal liability or sanction, disciplinary proceedings, retaliation or victimisation, including protection from adverse consequences for a person's security clearance, for making a disclosure

**Serious wrongdoing** includes

- a. An unlawful, corrupt or irregular use of public funds or public resources; or
- b. An act, omission or course of conduct that constitutes a serious risk to public health or public safety or the environment; or
- c. An act or omission or course of conduct that constitutes a serious risk to the maintenance of law, including the prevention, investigation, and detection of offences and the right to a fair trial; or
- d. An act or omission or course of conduct that constitutes an offence; or
- e. An act or omission or course of conduct by a public official that is oppressive, improperly discriminatory or grossly negligent or that constitutes gross mismanagement

## Process

### ***Who Can Make a Protected Disclosure?***

11. Under the Act, a protected disclosure may be made by any person who is or has been employed by the GCSB or NZSIS, including any contractor, secondee, volunteer, or any other person engaged to do work by the GCSB or NZSIS. The person must follow these internal procedures to make such a disclosure (as required by section 7 of the Act).

### ***What is a Protected Disclosure?***

12. A disclosure will be protected under the Act if:
  - a. It is about serious wrongdoing in or by the GCSB or the NZSIS; and
  - b. The employee or individual believes on reasonable grounds that the information is true or likely to be true; and
  - c. The employee or other person wants the serious wrongdoing to be investigated; and

- d. The employee or other person wants their disclosure to be protected.
13. The disclosure is still protected if the person is mistaken and the information is not about a serious wrongdoing, as long as the person making the disclosure believed on reasonable grounds that it was (see section 6 (3) of the Act). This is referred to in this policy as a good faith belief.
  14. A disclosure will still be covered by the Act even if there has been a “technical failure” to comply exactly with these internal procedures or the procedures set out in the Act, as long as the disclosure substantially complies with the requirements in paragraph 12 (section 6A of the Act). The person does not have to expressly refer to the Act when making a disclosure for it to be protected under the Act.
  15. A disclosure will **not** be considered a protected disclosure and protected under the Act if:
    - a. The employee or other person knows the information is false;
    - b. The employee or other person acts in bad faith in making the disclosure; or
    - c. The employee or other person did not believe on reasonable grounds that the information is about a serious wrongdoing; or
    - d. The information is protected by legal professional privilege.
  16. A disclosure that is trivial or misleading may not be considered a serious wrongdoing, and a disclosure about a trivial matter may be considered as acting in bad faith.

***How a Protected Disclosure Should be Made***

17. A disclosure should be made in accordance with the internal procedures set out in this policy.
18. It is the duty of the employee or other person wishing to make a protected disclosure to ensure, before making the disclosure, that the person to whom the disclosure is made holds the necessary security clearance and is authorised to have access to the information being disclosed. This includes the relevant SCI/ECI briefings if the disclosure relates to such material.
19. A disclosure may be made verbally or in writing. A disclosure made verbally will be subsequently confirmed in writing with the person making the disclosure.
20. A protected disclosure is considered to be made from the date of the disclosure, whether made verbally or in writing.

## **Who Disclosures May be Made to**

21. In the first instance, a protected disclosure should be made to one (or more) of the people designated in this policy approved to receive the disclosure. These people are:
  - a. Any Director of the GCSB or the NZSIS (second tier manager);
  - b. The GCSB or NZSIS Chief Legal Advisor;
  - c. The Chief Financial Officer;
  - d. The Chief People Officer;
  - e. The Director-General of the GCSB; or
  - f. The Director-General of the NZSIS.
22. The disclosure may be made about any topic to any of these people. It does not have to relate to their organisational responsibilities.
23. A disclosure may always be made directly to the Director-General if the person making the disclosure is concerned that any of the other people listed in this policy may either be involved in the alleged wrongdoing or by reason of any relationship it is not appropriate to disclose to them.
24. If the person is not sure whether the person has the necessary clearance or briefings to receive the information, then they should make the disclosure to the Director-General of the GCSB or the NZSIS.
25. In some specified circumstances, a protected disclosure may be made to the Inspector-General (who is the only Appropriate Authority for the GCSB and NZSIS), to the Minister responsible for an intelligence and security agency, or to the Prime Minister. See the section below on making a Disclosure Outside the GCSB or NZSIS.

## **Information to be Provided at Time of Disclosure**

26. The following information is helpful when making a disclosure and should be provided to the fullest extent possible:
  - a. Name and contact details of the person making the disclosure; and
  - b. The identity of the person or people believed to be involved or causing the serious wrongdoing; and
  - c. The nature of the serious wrongdoing ; and
  - d. Evidence of the serious wrongdoing, if available.
27. An anonymous disclosure may be made but it will make it more difficult to investigate and resolve. For this reason, the disclosure should provide as much information as possible.

28. The person making the disclosure may ask for confidential support at this time. This policy sets out the confidential support that may be offered to a person making a protected disclosure.

### ***Obligations on Recipient of a Protected Disclosure***

29. The person receiving the protected disclosure must do the following:

- a. Makes notes on the disclosure, if it is not made in writing, and check these are accurate with the discloser, including the date the disclosure is made; and
- b. Immediately inform the GCSB or NZSIS Chief Legal Advisor and their Director-General, unless they are the subject of the disclosure:
  - (i) If GCSB or NZSIS Chief Legal Advisor is the subject of the disclosure, the person receiving the disclosure will seek advice from Director Strategy, Governance and Policy, GCSB, or Deputy Director-General NZSIS, and the relevant Director-General who will undertake the assessment of the disclosure and consider whether to raise the matter with the Solicitor General.
  - (ii) If the Director-General is the subject of the disclosure, the person receiving the disclosure will seek advice from the Director Strategy, Governance and Policy, GCSB or Deputy Director-General NZSIS, and the relevant Chief Legal Advisor, who will then direct the investigation and make decisions (see below). They must also consider whether to raise the matter with the States Services Commissioner; and
- c. Go back to the person making the disclosure (preferably in writing) **within 5 working days** and:
  - (i) Let them know what action has been taken to assess the disclosure; and
  - (ii) Discuss any support requirements.

30. Where a disclosure is made that indicates an imminent threat to the life or safety of employees or others, the person receiving the disclosure must act on this information immediately. They must ensure the people who are responsible for taking action on any threat have the right information without delay.

### *Obligation of Confidentiality*

31. The person who receives the protected disclosure, and any person advised of the disclosure, have an obligation under the Act to use their best efforts to keep the identity of the person making the disclosure confidential, unless disclosure of the identity is essential to:
- a. An effective investigation of the allegations; or
  - b. To prevent serious risk to public health or public safety or the environment; or
  - c. Ensure the principles of natural justice can be followed.



32. This means that the identity of the person making the disclosures will be kept confidential to people who “need to know”.

33. The person making the disclosure may consent in writing to the disclosure of their identity and to whom it may be disclosed.

### ***Response to a Disclosure***

34. The Director-General (except where they are the subject of the disclosure), will appoint a person to provide advice on the matters set out below. This advice must be **provided within 15 working days** of the disclosure. The person appointed must be unbiased and impartial and have no management responsibility for the person making the disclosure and no management responsibility for the area covered by the disclosure.

35. The advice will include recommendations on:

- a. Whether the concern or disclosure may be considered a protected disclosure, or whether further investigation is required to determine this (i.e. whether it meets the criteria for serious wrongdoing and for protection under the Act); and
- b. Any immediate action required; and
- c. Whether there should be an investigation into the circumstances raised by the disclosure, and if so the terms of reference, timeframe, scope and who should be involved; and
- d. Any other matters the Director-General directs to be included

36. If the advice is that the disclosure is not about a serious wrongdoing, or if it is and no action is recommended, the report must include the reasons for this.

### ***Conduct of Any Investigation***

37. Any investigation must comply with the principles of natural justice, including:

- a. A final decision must only be made once all the parties involved or alleged to be involved have been given the opportunity to be made aware of the allegations and had the opportunity to be heard on the allegations;
- b. All parties involved in the investigation must be
  - i. given reasonable notice of any interview;
  - ii. advised that they may have legal representation and/or a support person in any interview; and
  - iii. given a reasonable opportunity and period of time to respond to any allegations.

38. Any investigation must result in a written report for the Director-General, with recommendations for response.

### ***Decision and Response***

39. The Director-General (or other person responsible if the disclosure concerns the Director-General) is responsible for deciding whether the disclosure involves a serious wrongdoing, and the actions to be taken in response, including further investigation. The Director-General may seek further information after the receipt of the advice, pursuant to paragraph 37 above, may direct further investigation, or may make a final decision on the response to the protected disclosure.
40. Where the Director-General is the subject of the disclosure, the decision will be made by the people appointed to do so (see paragraph 29 (b) of this policy).

### ***Advice to Person Disclosing***

41. It is recommended that the person making the disclosure is advised when the advice is first provided to the Director-General for consideration. This is to ensure that they are fully aware that action to consider their disclosure is taking place and the matter is now with a decision maker and that this has occurred within 20 working days of them making the disclosure (see section 9 (c) of the Act).
42. The person making the disclosure should be advised of the outcome of the final decision. This should include advice on whether the disclosure was considered to be a protected disclosure and what actions, if any, will be taken. The Director-General will decide how much detail will be provided to the person making the disclosure.
43. If an investigation taking some time is required, it is recommended that the person making the disclosure should be updated on progress at least **monthly**.

### ***When the Matter is Not a Serious Wrongdoing***

44. If, after receiving advice, the Director-General (or other person where the Director-General has been the subject of the disclosure) decides that the protected disclosure is not about serious wrongdoing, and is therefore not considered a protected disclosure, the Director-General is responsible for ensuring the person making the disclosure is advised of the outcome of the decision and offered the appropriate support to assist them in dealing with their concerns. This includes putting in place any measures needed to protect the integrity of classified information. Advice on any measures may be sought from the Assistant Director of Security Services Group.

## Protections for Persons Making a Disclosure

45. A person is entitled under the Act to protection when making a protected disclosure as long as it meets the criteria in paragraphs 11 and 12 above, regardless of whether any action is taken in response. The GCSB and NZSIS will provide confidential support for a person who makes a protected disclosure and ensure that disclosures may be made without fear of reprisal or repercussions.

### *Immunity From Civil or Criminal Proceeding Associated With Making a Disclosure*

46. A person who makes a protected disclosure, or refers a protected disclosure to the Inspector-General for investigation, Minister responsible for an intelligence and security agency or the Prime Minister (in accordance with the section below), is protected from civil or criminal proceedings for having made the disclosure or referral.
47. However, if the person making the disclosure has been involved in the serious wrongdoing themselves, while the making of the disclosure may be protected, they may not be protected from any justified disciplinary action, security measure or criminal process in relation to that serious wrongdoing.
48. The protections conferred by the Act do not apply where the person who makes a disclosure of information makes an allegation known to that person to be false or otherwise makes the disclosure in bad faith.

### *Confidentiality*

49. The person making the disclosure is entitled to have their identity kept confidential to the people who “need to know” and may only be shared with others where disclosing the identity is essential to carrying out any investigation, essential to prevent a serious risk to public health and safety or the environment, or essential to ensure the principles natural justice are followed. See also section above on Obligations on Recipient of a Protected Disclosure.

### *Protection from Retaliation and Victimization*

50. A person making a disclosure is protected by law from retaliation or victimisation as a result of making, or intending to make, a disclosure.
51. The Act provides protections against retaliation, where retaliation means dismissal or disadvantage by some unjustifiable action by the agency (as defined in section 103 of the Employment Relations Act 2000).
52. The Human Rights Act 1993 (HRA) provides protection against victimisation. Under section 66 of the HRA, it is unlawful to treat or threaten to treat any person less favourably because they have exercised their rights under the Protected Disclosures Act.

- ██████████
53. Where any discloser considers that they have been treated less favourably or suffered some disadvantage because of the fact that they have made, or intend to make, a disclosure, they should discuss this in the first instance with the Chief People Officer or the Director-General.
  54. An existing employee may lodge a personal grievance under the Employment Relations Act 2000 if they experience retaliatory action because they have made or intend to make a disclosure.
  55. People other than existing employees should refer to the terms of their contract or other terms of engagement for remedies for retaliation.
  56. Any person, including employees, contractors and secondees, making a disclosure who experiences victimisation as a result of making or proposing to make a disclosure may complain to the Human Rights Commissioner under the HRA.
  57. An employee can only take one course of action when seeking a remedy to retaliation or victimisation and must choose between action under the Employment Relations Act or the Human Rights Act.

### ***Security Clearance***

58. A person who makes a protected disclosure is also protected from adverse consequences (from making the disclosure) for their security clearance. For existing employees, if it occurs, it may be grounds for taking a personal grievance.

### **Support for Person Making a Disclosure**

59. The GCSB and NZSIS will offer support as appropriate to any person who has made a protected disclosure. Support may include access to EAP, a short period of leave from work, re-location, or other support that may be appropriate (noting that some of these measures may require discussion with other senior managers and the Chief People Officer, as long as the person making the disclosure has provided their consent for this purpose).
60. If a disclosure is made in good faith but is not considered by the Director-General to be about a serious wrongdoing, the GCSB or the NZSIS will make their best efforts to ensure that the concerns raised are kept confidential and the person is provided with support to address the issues they are concerned about.
61. In this instance, the person will be given the opportunity to discuss their concerns with their manager, or another senior person. Consideration should be given to whether a support programme should be put in place. For instance, referral to the EAP and/or authorised counselling services. Other support measures may be considered on a case by case basis.

## Making a Disclosure Outside the GCSB or NZSIS

62. A person must not make disclosures of classified information or information relating to the activities of an intelligence and security agency to anyone outside the GCSB or the NZSIS, other than the Inspector-General (who is the only Appropriate Authority for the GCSB and NZSIS), the Minister responsible for an intelligence and security agency, or the Prime Minister, and only in the circumstances described below. The protections of the Act do not cover instances of making the disclosure outside these processes, for instance to other external parties.
63. This means that a disclosure involving classified information or any information relating to the activities of the GCSB or the NZSIS cannot be made to other any other authority, including any other Ombudsmen, any other Commissioner of Police, or any other Minister of the Crown.
64. This policy sets out the circumstances where it is permitted to make a disclosure directly to the Inspector-General, or the Minister responsible for an intelligence and security agency, or the Prime Minister.

### ***Making a Disclosure to the Inspector-General***

65. The Inspector-General is the only Appropriate Authority for the GCSB and NZSIS. The Act provides that, in some specific circumstances, a disclosure may be made directly to the Inspector-General without first making a disclosure to the GCSB or NZSIS.

#### *A direct disclosure*

66. A disclosure may only be made directly to the Inspector-General without disclosing first to a person in the GCSB or NZSIS, if the person believes on reasonable grounds that:
- The Director-General is or may be involved in the serious wrongdoing ; or
  - Immediate reference to the Inspector-General is justified by reason of the urgency of the matter or some other exceptional circumstance.

#### *After having already made a disclosure to GCSB or NZSIS*

67. A person may also refer a disclosure to the Inspector-General if they have already made a disclosure to someone within GCSB or NZSIS if the person making the disclosure believes there has been no action or recommended action in relation to the disclosure after 20 working days.
68. In both of these situations, the person should follow the procedures set out on the Inspector-General's website and in the Act.

## ***Making a Disclosure to a Minister Responsible for an Intelligence and Security Agency or the Prime Minister***

69. A person may only refer a disclosure to the Minister responsible for an intelligence and security agency or the Prime Minister if the person making the disclosure has already made substantially the same disclosure to someone within GCSB or NZSIS and/or to the Inspector-General in accordance with the Act. In order to make this disclosure they must:
- a. Believe on reasonable grounds that the Director-General (or person in the GCSB or NZSIS responsible for the investigation and decision), or the Inspector-General, has:
    - i. Decided not to investigate the matter; or
    - ii. Has decided to investigate the matter but has not made progress with the investigation within a reasonable time after the date on which the disclosure was made; or
    - iii. Has investigated the matter but has not taken any action in respect of the matter nor recommended the taking of action in respect of the matter as the case may be; and
  - b. Continue to believe on reasonable grounds that the information disclosed is true or likely to be true.

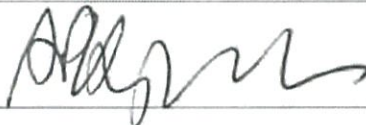
## **Further Information and Guidance**

70. Any person may get further information from:
- a. The Chief Legal Advisor for GCSB or NZSIS;
  - b. The Managers of Compliance and Policy of GCSB and NZSIS;
  - c. The Chief People Officer for the GCSB and NZSIS; or
  - d. The Inspector-General.
71. This information can be provided on a confidential basis and may be obtained at any stage of the process.
72. Further information and guidance on making a protected disclosure can be found on
- a. the GCSB intranet, on the NZSIS intranet;
  - b. on the Office of Inspector-General of Intelligence and Security's website [www.igis.govt.nz](http://www.igis.govt.nz); and
  - c. and on the States Services Commission website under their "Speaking Up" material [www.ssc.govt.nz/speaking-state-services](http://www.ssc.govt.nz/speaking-state-services)

## Previous Policy Revoked

- 73. This policy revokes and replaces the GCSB Policy Statement PS-1002 *Protected Disclosures Act 2000 GCSB Internal Procedures*, which was approved on 16 January 2012.
- 74. This policy revokes and replaces the NZSIS policy: Protected Disclosures Act 2000 NZSIS whistleblowing procedures.

## Approval

Approved by:	Director-General GCSB		
Approval date:	27/7/18		
Effective date:			
Policy Owner:	Director, Strategy, Governance and Performance		
Current incumbent:	s6(a)		
Policy Administrator:	Compliance and Policy Manager		
Current incumbent:	s6(a)	Contact number:	s6(a)

Approved by:	Director-General NZSIS		
Approval date:	26/7/18		
Effective date:			
Policy Owner:	Deputy Director-General		
Current incumbent:	s6(a)		
Policy Administrator:	Manager, Compliance and Risk		
Current incumbent:	s6(a)	Contact number:	s6(a)



### Summary of Minor Amendments

Date	Summary of changes	Approval Authority	Signature



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI



New Zealand  
Security Intelligence  
Service  
Te Pā Whakamarumaru

## Joint Policy Statement: JPS-006

# Human rights risk management policy

<b>Policy Owner</b>	Chief Legal Adviser, GCSB Chief Legal Adviser, NZSIS
<b>Policy Administrator</b>	Legal Adviser, GCSB Legal Adviser, NZSIS
<b>Approval Authority</b>	Director-General, GCSB Director-General, NZSIS
<b>Approval Date</b>	28 September 2017
<b>Review Date</b>	31 March 2019

## Contents

Purpose .....	3
Scope .....	3
Definitions .....	3
Background .....	5
Ministerial policy statement on co-operation with overseas public authorities.....	6
Policy.....	6
Human rights risk approval required before taking action.....	6
Who may grant human rights risk approvals .....	7
Matters to be identified in applications for human rights risk approvals.....	7
Human rights risk reviews required after receiving certain information.....	8
Who must sign off human rights risk reviews .....	9
Matters to be identified in human rights risk reviews .....	9
Approved parties .....	10
Matters to identify when seeking ministerial approval of governments and foreign public agencies .....	11
Criteria for approval of non-government entities and individuals .....	12
Approved information.....	12
Actions where human rights breaches are suspected or confirmed .....	12
Appendix 1: Human rights risk assessment process .....	14
Appendix 2: Torture and similar mistreatment.....	17
Appendix 3: Requirements of ministerial policy statement.....	18
Approvals .....	20
GCSB Approval .....	20
NZSIS Approval .....	20
Summary of Minor Amendments.....	21

## Purpose

1. This policy statement sets processes that GCSB and NZSIS will use to manage the risk of contributing to actions by foreign parties that may **breach human rights**.
2. This policy statement does not define when or how GCSB and NZSIS will interact with foreign parties. Relevant personnel in each agency will make decisions about when and how to interact with foreign parties while following the processes in this policy statement.

## Scope

3. This policy applies to all interactions GCSB or NZSIS (including employees, secondees **6(a)**) have with **foreign parties**. This includes:
  - a. providing intelligence and analysis to a foreign party;
  - b. providing protective security services, advice, or assistance to a foreign party;
  - c. co-operating with a foreign party (including receiving services or assistance from that party); and
  - d. receiving information from a foreign party.
4. Foreign parties:
  - a. include foreign governments and their agencies, non-government entities to the extent they operate outside New Zealand, and New Zealand citizens and permanent residents who act for or on behalf of a foreign government, entity, or person, or a designated terrorist entity;
  - b. do not include New Zealand citizens or permanent residents (other than those in a. above) or persons who work for the New Zealand Government (such as secondees or **6(a)**)
5. The relevant Director-General may authorise variations to this policy for specific purposes in order to comply with any ministerial requirements for interacting with foreign parties.

## Definitions

6. The following definitions are used in this policy statement.
  - a. **Approved information** means a category of information approved by the relevant Director-General (see paragraphs 41 to 42). Approved information does not need the subject of **human rights risk approvals** (see paragraph 16.e.-f.).

- b. **Approved party** means a party that has been approved by a relevant approval authority (see paragraphs 32 to 40). Individual interactions with approved parties and NZSIS do not usually need to be the subject of **human rights risk approvals** or **human rights risk reviews** (see paragraph 16.a.-d.).
- c. **Human rights risk approval** means approval to take certain actions with foreign parties that must be granted before GCSB or NZSIS take those actions (see paragraphs 15 and 16). The persons who may grant an approval depends on the risk of human rights breaches, as identified through a **human rights risk assessment**.
- d. **Human rights risk review** means a review to assess the risk that information was obtained by human rights breaches that must be carried out after receiving information from a foreign party where there was no reasonable prior opportunity to carry out a human rights risk assessment, subject to some exceptions (see paragraph 24 and 25). The persons who may sign-off a review depends on the risk of human rights breaches, as identified through a **human rights risk assessment**.
- e. **Human rights risk assessment** means the process for determining the risk of **human rights breaches** associated with an interaction with a foreign party (set out in **Appendix 1**).
- f. The **ISA** means the Intelligence and Security Act 2017.
- g. **NZBORA** means the New Zealand Bill of Rights Act 1990.
- h. **Human rights breaches** means any unlawful breach of human rights obligations recognised by New Zealand law, and includes:
  - i. rights to life and security of the person (see sections 8 to 11 of NZBORA), including rights against **torture and similar mistreatment**;
  - ii. democratic and civil rights (see sections 12 to 18 of NZBORA);
  - iii. non-discrimination and minority rights (see sections 19 and 20 of NZBORA);
  - iv. rights relating to search, arrest, and detention (see sections 21 to 27 of NZBORA).
- i. **Torture and similar mistreatment** means the following (also see **Appendix 2**):
  - i. an act of torture, as defined in section 2(1) of the Crimes of Torture Act 1989; and

- ii. cruel, degrading, or disproportionately severe treatment or punishment.
7. Information about the meaning of the terms **contribute to, general possibility, specific indication, and mitigate** are in **Appendix 1**.

## Background

8. GCSB and NZSIS may lawfully provide information to and co-operate with certain foreign parties as part of performing their statutory functions. The scope of this depends, in some cases, on the existence and terms of authorisations issued by the Minister responsible for each agency (see section 10, 11 and 12 of the **ISA**). GCSB and NZSIS may also lawfully receive information from foreign parties when performing their functions.

### *Domestic legal requirements to act consistently with human rights*

9. GCSB and NZSIS must act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. Further, when authorising GCSB or NZSIS to provide information, the Minister responsible for the agencies is required to be satisfied, that in providing that information, GCSB or NZSIS will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
10. Human rights are recognised in New Zealand law through legislation such as the New Zealand Bill of Rights Act 1990, the Human Rights Act 1993, and the Crimes of Torture Act 1989, and in case law.
11. GCSB and NZSIS personnel may be liable for criminal offences if they are involved in certain actions that **breach human rights**. Legal action can also be taken against the government for **human rights breaches**.

### *International law applicable to human rights*

12. New Zealand has obligations under international law to respect certain human rights. These international legal obligations arise from treaties that New Zealand is a state party to, or from customary international law. Treaties that create international legal obligations to protect human rights include the United Nations Convention Against Torture and the International Covenant on Civil and Political Rights.
13. GCSB and NZSIS personnel may also be liable for breaches of international criminal law if they are involved in certain actions that **breach human rights**.

## Ministerial policy statement on co-operation with overseas public authorities

14. The Ministerial policy statement “cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities” contains principles and requirements about interacting with certain foreign parties consistently with human rights recognised by New Zealand law. Relevant requirements of that MPS are in **Appendix 3** and are incorporated into this policy statement.

## Policy

### Human rights risk approval required before taking action

15. GCSB or NZSIS will only take the following actions after a **human rights risk approval** has been granted (subject to the exceptions in paragraph 16).
- a. Provide information to a foreign party.
  - b. Grant permission for another party to provide information to a foreign party.
  - c. Co-operate with a foreign party.
  - d. Accept information from a foreign party where there is a reasonable opportunity to carry out a human rights risk assessment.
16. GCSB and NZSIS may take any of the following actions without a **human rights risk approval** being granted.
- a. Provide information to an **approved party**, unless there is a **specific indication** that providing the information will contribute to a breach of human rights.
  - b. Grant permission for another party to provide information to an **approved party**, unless there is a **specific indication** that providing the information will contribute to a breach of human rights.
  - c. Co-operate with an **approved party**, unless there is a **specific indication** the co-operation or the results of the co-operation will contribute to a breach of human rights.
  - d. Accept information from an **approved party**, unless there is a **specific indication** the information was obtained through a breach of human rights.
  - e. Provide **approved information** to any party.
  - f. Grant permission for another party to provide **approved information** to any party.

### ***Who may grant human rights risk approvals***

17. The following persons may grant a **human rights risk approval**, as determined by the risk category of the proposed action.

<b><i>Risk category</i></b>	<b><i>Risk description</i></b>	<b><i>Minimum approval authority</i></b>
Category 1	Substantial likelihood of <b>torture or similar mistreatment</b> (mitigated or unmitigated).	Minister
Category 2	Unmitigated substantial likelihood of breaches <b>not involving torture or similar mistreatment</b> .	Minister
Category 3	Mitigated substantial likelihood of breaches <b>not involving torture or similar mistreatment</b> .	Director-General
Category 4	Speculative likelihood of any <b>human rights breach</b> .	Tier 3 Manager or delegated officer as approved by a Director-General
Category 5	Negligible likelihood of any <b>human rights breach</b> .	Any manager

18. The **human rights risk assessment** process must be used to determine the risk category of the proposed action.
19. If GCSB or NZSIS are unable to apply the risk assessment process in relation to a proposed action (for example, due to a lack of information to assess relevant matters), the action must be approved as if there were a category 1 risk.

### ***Matters to be identified in applications for human rights risk approvals***

20. All applications for **human rights risk approvals** must be recorded in writing (either at the time, or as soon as possible after the approval is granted if done in urgent circumstances). All applications for approvals must identify:
- a. the risk description applicable to the approval, as determined using the **human rights risk assessment** process;
  - b. the particular human rights that may be breached (if any);
  - c. any relevant legal obligations under New Zealand law or international law and other relevant international obligations; and



- d. the purpose of taking the proposed action.
21. All applications for category 1, 2 and 3 **human rights risk approvals** must also advise the approval authority of:
- a. the risk of employees of GCSB or NZSIS committing an offence against New Zealand or international criminal law if the proposed action occurs;
  - b. the risk of GCSB or NZSIS breaching New Zealand law if the proposed action occurs; and
  - c. the risk of New Zealand being responsible for an wrongful act under international law if the proposed action occurs.
22. All applications for category 1 human rights risk approvals must also advise the Minister of any factors that mitigate the likelihood of human rights breaches

***Consequences of granting a human rights risk approval***

23. By granting a **human rights risk approval**, the approval authority:
- a. confirms the applicable risk description; and
  - b. approves the proposed action in light of the identified risk of the proposed action contributing to a breach of human rights and associated legal risks.

**Human rights risk reviews required after receiving certain information**

24. GCSB and NZSIS must carry out a **human rights risk review** after receiving information from a foreign party where there was no reasonable prior opportunity to carry out a human rights risk assessment (subject to the exception in paragraph 25). The **human rights risk review** must be signed off as soon as practicable after the information is received.
25. GCSB and NZSIS are not required to carry out a **human rights risk review** after receiving information from an **approved party**, unless there is a **specific indication** the information was obtained as a result of a breach of human rights.

### Who must sign off human rights risk reviews

26. The following persons must sign off **human rights risk reviews**, as determined by the risk category that applies to the received information.

<i>Risk category</i>	<i>Risk description</i>	<i>Minimum approval authority</i>
Category 1	Substantial likelihood of <b>torture or similar mistreatment</b> (mitigated or unmitigated).	Minister
Category 2	Unmitigated substantial likelihood of breaches not involving <b>torture or similar mistreatment</b> .	Minister
Category 3	Mitigated substantial likelihood of breaches not involving <b>torture or similar mistreatment</b> .	Director-General
Category 4	Speculative likelihood of any <b>human rights breach</b> .	Tier 3 Manager or delegated officer as approved by a Director-General
Category 5	Negligible likelihood of any <b>human rights breach</b> .	Any manager

27. The **human rights risk assessment** process must be used to determine the applicable risk category.

28. If GCSB or NZSIS are unable to apply the risk assessment process in relation to a proposed action (for example, due to a lack of information to assess relevant matters), the review must be signed off, at a minimum, as if it were a category 4 risk.

### Matters to be identified in human rights risk reviews

29. All **human rights risk reviews** must be recorded in writing. All reviews must identify:

- a. the risk category of the review, as determined using the **human rights risk assessment** process; and
- b. the particular human rights that may have been breached (if any).

30. All category 1, 2 and 3 **human rights risk reviews** must also:

- a. confirm whether GCSB or NZSIS suspect the information received was obtained by a human rights breach (meaning the actions in paragraph 44 are required);

- b. identify the risk of employees of GCSB or NZSIS committing an offence against New Zealand or international criminal law if similar information is received in the future;
- c. identify the risk of GCSB or NZSIS breaching New Zealand law if similar information is received in the future;
- d. identify the risk of New Zealand being responsible for a wrongful act under international law if similar information is received in the future;
- e. the purpose of any further receipt of the same type or information or of further interaction with the same party; and
- f. identify what actions, if any, are to be taken in relation to the information received, any further receipt of the same type of information, or of further interaction with the same party.

**Consequences of granting a human rights risk approval**

- 31. By signing off a **human rights risk review**, the approval authority:
  - a. confirms the applicable risk description;
  - b. determines actions (if any) to be taken to ensure GCSB or NZSIS do not breach the law through interaction in future.

**Approved parties**

- 32. The 6(a) are approved parties.
- 33. The following persons may approve other foreign parties as **approved parties**.

<i>Type of foreign party</i>	<i>Minimum approval authority</i>
Governments and foreign public agencies	Minister
Non-government entities.	Tier 3 Manager or delegated officer as approved by a Director-General
Individuals	Tier 3 Manager or delegated officer as approved by a Director-General

- 34. Applications for approved parties must include all relevant information that is reasonably available. See paragraph 7 of **Appendix 1** for guidance about some sources of information.
- 35. All approvals of approved parties must be recorded in writing. Approvals will last for three years unless revoked, and may be renewed.

36. Note:

- a. having **approved party** status does *not* automatically mean GCSB or NZSIS have *legal* authority to interact with the party (such as under a relevant ministerial authorisation);
- b. a party identified in another legal instrument (such as in a ministerial authorisation or intelligence warrant) is *not* automatically an **approved party** because it is identified in that instrument;
- c. the relevant legal team should be consulted if it is unclear whether GCSB or NZSIS has legal authority to interact with a party;
- d. the relevant policy and compliance team should be consulted if it is unclear whether a party is an **approved party**.

***Matters to identify when seeking ministerial approval of governments and foreign public agencies***

37. When seeking approval for governments and foreign public agencies to become approved parties, GCSB and NZSIS must advise the Minister of the following matters.
  - a. The likelihood of the government or agency for which approval is sought:
    - i. using information provided by GCSB or NZSIS in actions that would **breach human rights**;
    - ii. breaching human rights when co-operating with GCSB and NZSIS or in the use of any results of that co-operation; or
    - iii. obtaining information by methods that **breach human rights**.
  - b. Any significant international human rights treaties that the government has not signed or ratified, or signed with reservations that substantially limit protections of human rights.
  - c. Mechanisms available to GCSB, NZSIS and the broader New Zealand Government to identify and seek information about any **human rights breaches** that could be caused by the government or agency.
38. The likelihood of the matters in paragraph 37.a. must be assessed using the **human rights risk assessment** process.

### **Criteria for approval of non-government entities and individuals**

39. A non-government entity or an individual may only be an **approved party** if the approval authority assesses that the party will not:
- a. use information provided by GCSB or NZSIS in actions that would **breach human rights**;
  - b. **breach human rights** when co-operating with GCSB and NZSIS or in the use of any results of that co-operation; or
  - c. obtain information by methods that **breach human rights**.
40. The following matters must be considered before approving a non-government entity or an individual.
- a. Whether the entity or individual is known to work with a foreign government to take action (including disclosing information) that may support actions that **breach human rights**.
  - b. Mechanisms available to GCSB, NZSIS and the broader New Zealand Government to identify and seek information about any **human rights breaches** that could be caused by the entity or individual.

### **Approved information**

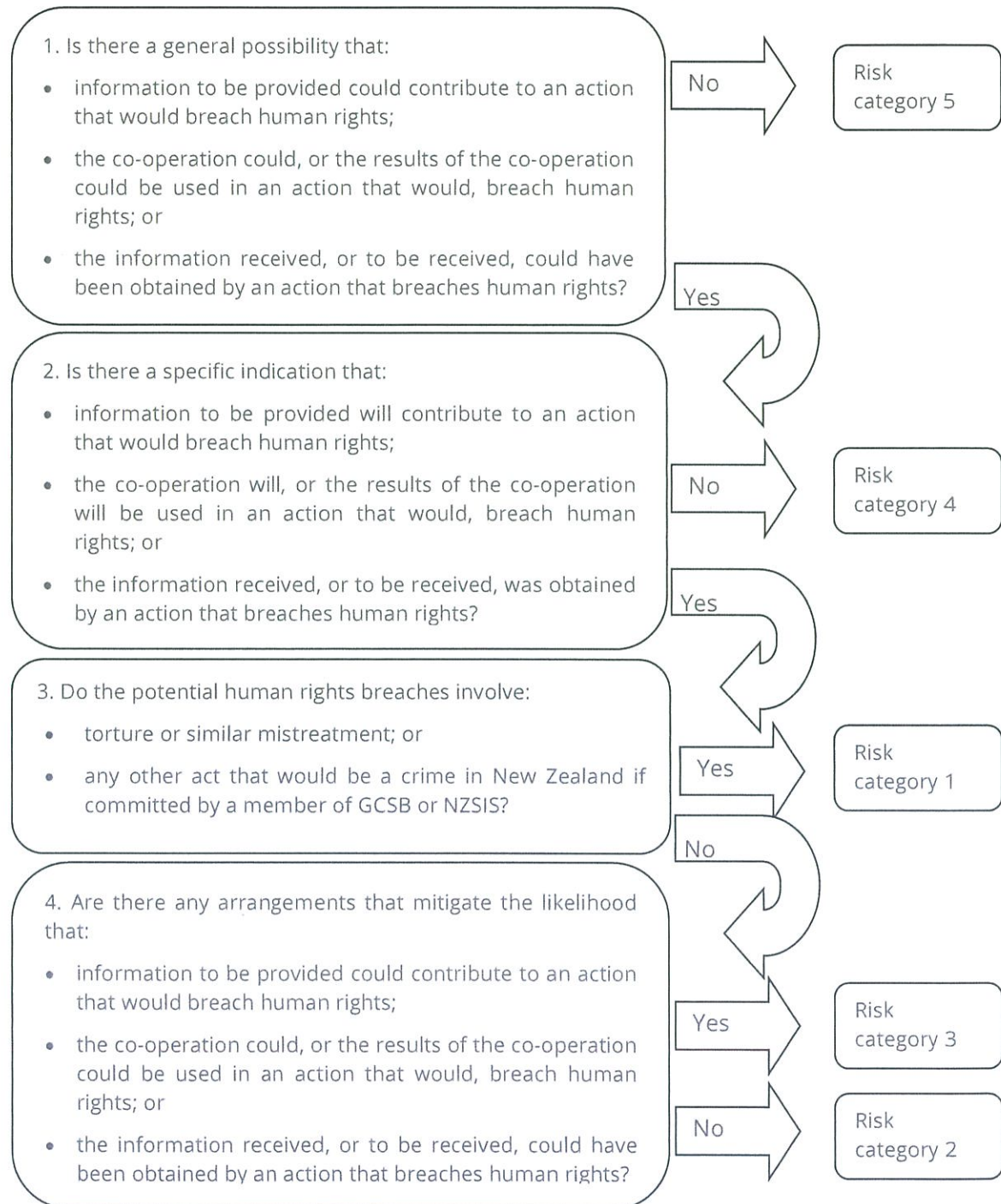
41. The Director-General of GCSB or NZSIS may approve a category of information as **approved information** if there is no **general possibility** that providing the information to any foreign party would **contribute to** an action that breaches human rights (meaning the information would always be assessed to fall into risk category 5 in the **human rights risk assessment** process).
42. All approvals of **approved information** must be recorded in writing. Approvals will last for three years unless revoked, and may be renewed.

### **Actions where human rights breaches are suspected or confirmed**

43. The actions in paragraph 44 must be taken if GCSB or NZSIS suspect or confirm:
- a. information that GCSB or NZSIS provided to a foreign party (including an approved party) has been used in an action that **breached human rights**;
  - b. co-operation by GCSB or NZSIS with a foreign party (including an approved party), or the results of that co-operation were used in an action that, **breached human rights**; or
  - c. information from a foreign party (including an approved party) was obtained by an action **that breaches human rights**.

44. GCSB and NZSIS must:
- a. seek legal advice;
  - b. investigate, to the extent practicable, the suspected breaches of human rights;
  - c. advise the responsible Minister and the Inspector-General of Intelligence and Security;
  - d. advise the Ministry of Foreign Affairs and Trade and, as appropriate, other relevant New Zealand Government entities; and
  - e. stop or restrict ongoing work with parties potentially responsible for the suspected human rights breach;
  - f. decide, alongside other appropriate New Zealand Government entities, whether to take any actions to mitigate the **human rights breaches** that have occurred.

## Appendix 1: Human rights risk assessment process



1. The following paragraphs provide more information about the meaning of terms for carrying out **human rights risk assessments**.
2. GCSB or NZSIS actions **contribute to** an action by a foreign party that breaches human rights if there is a clear causative link between the GCSB or NZSIS action and the action by the foreign party that breaches human rights. For example:
  - a. providing a phone number to a foreign government is considered to contribute to a breach of human rights if that phone number is used (with no further information) to identify the location of a person who is then detained and interrogated in a way that breaches human rights;
  - b. providing intelligence about the alias of an unknown person is not considered to contribute to human rights breaches if the recipient of the intelligence carries out analysis based on that intelligence and a range of other information to identify, locate, and subsequently breach the human rights of that person.
3. There is a **general possibility** of a human rights breach if that breach could logically occur and there is a genuine basis for believing that a relevant party could seek to take actions that would cause such a breach. For example:
  - a. there would be a general possibility of information sharing **contributing to human rights breaches** if the information relates to the location of suspected terrorists in a country and is being shared with a government agency of that country that is known to seek to detain terrorist suspects and **breach human rights** when interrogating detainees;
  - b. there is not a general possibility of information sharing leading to **human rights breaches** if the information is of a character that sharing it could not **contribute to** such breaches.
4. There is a **specific indication** of a human rights breach if there is specific and reliable information that one or more relevant parties could seek to take actions that would cause such a breach in the particular circumstances.
  - a. Using the scenario in paragraph 3.a, there will be a specific indication of the information sharing leading to human right breaches if there is intelligence reporting that the recipient agency may seek to detain and interrogate the person.
5. Arrangements will **mitigate** the likelihood of a human rights breach if they logically affect the ability or willingness of relevant persons to take those actions and those persons are not realistically likely to circumvent the arrangements. Examples of arrangements that may mitigate the likelihood of breaches are:



- a. reliable assurances from the recipient (either to GCSB or NZSIS directly, or another party) about how the co-operation or information will be used or how the information to be received was obtained;
  - b. caveats on the use of information; and
  - c. mechanisms to monitor or review compliance with human rights standards (including visits to persons who may have been detained as a result).
6. The following factors may be relevant when carrying out **human rights risk assessments**:
- a. the human rights record of the party;
  - b. domestic laws protecting human rights applicable to the party;
  - c. whether a government has ratified relevant human rights treaties and any reservations that fundamentally affect the protected rights;
  - d. any mechanisms to investigate human rights breaches in the relevant country; and
  - e. whether there is an independent judiciary with jurisdiction to hear cases related to human rights breaches.
7. GCSB and NZSIS must use all information reasonably available in the circumstances when carrying out the **human rights risk assessment** process (including classified information).
- a. Reasonable efforts should be taken to obtain relevant information from the Ministry of Foreign Affairs and Trade to inform **human rights risk assessment**.
  - b. Common sources of information include:
    - i. information published by foreign governments (for example, US State Department Human Rights Reports);
    - ii. information published by credible non-governmental organisations; and
    - iii. intelligence reports.

## Appendix 2: Torture and similar mistreatment

1. This appendix provides more detail about terms referred to in the definition of **torture or similar mistreatment**.
2. Section 2(1) of the Crimes of Torture Act 1989 defines an "act of torture" as:

*any act or omission by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person –*

*(a) for such purposes as –*

- (i) obtaining from that person or some other person information or a confession; or*
- (ii) punishing that person for any act or omission for which that person or some other person is responsible or is suspected of being responsible; or*
- (iii) intimidating or coercing that person or some other person; or*

*(b) for any reason based on discrimination of any kind; -*

*but does not include any act or omission arising only from, or inherent to, any lawful sanctions that are not inconsistent with the Articles of the International Covenant on Civil and Political Rights*

3. Cruel, degrading, or disproportionately severe treatment or punishment includes any act or omission by which severe pain or suffering, whether physical or mental, is intentionally inflicted on person (but without the purposes in paragraph (a) of the definition of "act of torture" above).
4. Examples of practices that may amount to torture, cruel, degrading, or disproportionately severe treatment or punishment include:
  - a. sleep deprivation;
  - b. physical abuse or punishment of any sort; and
  - c. withdrawal of food, water or medical help.

### Appendix 3: Requirements of ministerial policy statement

1. The ministerial policy statement “cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities contains the following requirements relevant to this policy (in addition to those explicitly in the ISA).
2. 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 interactions with overseas public authorities (paragraph 59).
3. For all interactions with overseas public authorities, GCSB must have internal policies in place that ensure they act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law (paragraph 32).
4. GCSB and NZSIS should have regard to New Zealand’s human rights obligations at international law (paragraph 31).
5. GCSB and NZSIS must assess the likelihood of human rights breaches occurring or having occurred in connection with any interaction with overseas public authorities (paragraph 37).
6. GCSB and NZSIS must reassess any interactions with overseas public authorities where there is a real risk that the activity will lead to or has been obtained as a result of human rights breaches, and must not interact with the party in the meantime (paragraph 36).
7. When considering a proposal for a ministerial authorisation from GCSB or NZSIS, the Minister may be satisfied that GCSB and NZSIS will act consistently with human rights obligations recognised by New Zealand law on the basis of the processes the agencies will use to assess human rights practices of the overseas public authorities (paragraphs 40 and 62).
8. GCSB and NZSIS assessments of human rights practices and decisions to interact must be based on certain factors (paragraphs 38, 41, 42 and 63).
9. The Minister may set conditions on certain interactions and will specify thresholds of risk at which decisions must be referred back to the Minister (paragraphs 43 and 64).
10. For interaction with overseas public authorities that do not normally require ministerial authorisation, GCSB and NZSIS must have clear levels of decision-making with approval levels that vary according to certain risks. GCSB and NZSIS must obtain ministerial authorisation for these interactions at agreed levels – in particular if is a reasonable basis for concern about a country’s human rights record or the interaction might involve complicity in those breaches (paragraphs 45 and 65).

---

Joint Policy Statement - 006

Page: 18 of 21

---

Human rights risk management policy


Version: 1.0

Date: 28/9/2017

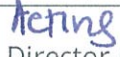
11. GCSB and NZSIS may pass certain unsolicited information they suspect was obtained by human rights breaches to relevant enforcement agencies where there is a credible risk to New Zealand's national security or a risk to the safety of New Zealanders (paragraph 47).
12. GCSB and NZSIS must immediately suspend interaction with an overseas public authority (and others related to it) where GCSB or NZSIS may have been complicit in human rights breaches by that party (paragraphs 46 and 66).
13. GCSB and NZSIS must notify certain New Zealand parties of suspected human rights breaches in some situations (paragraphs 46, 47 and 66).

## Approvals

### GCSB Approval

Approved by:	Director-General, GCSB	
Approval date:	28 September 2017	
Policy Owner:	Chief Legal Adviser, GCSB	
Current incumbent:	s6(a)	
Policy Administrator:	Legal Adviser, GCSB	
Current incumbent:	s6(a)	Contact number: s6(a)

### NZSIS Approval

Approved by:	 Director-General, NZSIS	s6(a)
Approval date:	28 September 2017	
Policy Owner:	Chief Legal Adviser, NZSIS	
Current incumbent:	s6(a)	
Policy Administrator:	Senior Legal Adviser, NZSIS	
Current incumbent:	s6(a)	Contact number: s6(a)

**Effective date: 28 September 2017**

**Review date: 31 March 2019**

## Summary of Minor Amendments

Date	Summary of changes	Approval Authority	Signature

## Summary: Sensitive Category Individuals Policy

*Summary prepared under section 16(1)(e) of the OIA, in order to protect the interests of section 6(a). Policy superseded on 29 July 2021.*

### Introduction

The legislative and compliance framework the NZSIS operates within requires the agency to have policies in place to ensure operational collection activity involving sensitive category individuals is appropriately authorised and managed.

The relevant policy outlines the types of individuals and situations the agency considers sensitive and sets expectations for managing the risks involved.

The policy applies to situations where the subject of the information or activity is a sensitive category individual, or where a sensitive category individual is not the subject but may be indirectly affected by agency activities.

Journalists are included in the definition of a sensitive category individual.

### Policy

#### *Scope*

NZSIS staff must follow this policy when planning, approving and conducting investigative or operational activity about or directly involving sensitive category individuals. The policy also applies to situations where it can be reasonably anticipated such individuals could be involved.

The investigative or operational activity must be lawful, necessary and proportionate to the performance of the NZSIS's functions. Alternative ways of obtaining the information should be considered where possible.

Staff must be alert to any factors that may increase the likelihood of encountering a sensitive category individual or their data, as sometimes staff will not know they are interacting with a person in this category.

Reasonable efforts using already available information must be made to determine if investigative or operational activity is being conducted about, or directly involves, a sensitive category individual. Staff must not however, undertake further intrusive activity for the sole purpose of making that assessment.

#### *Post-collection identification*

If a person is identified as a sensitive category individual after collection, the continuation of the activity or the use of the information must be approved in accordance with this policy. If the information is irrelevant, it should be destroyed.

#### *Authorisation*

The policy establishes a regime that must be followed for authorising any investigative or operational activity against sensitive category individuals. Staff must ensure that any activity involving a sensitive category individual is appropriately authorised using the framework established in the policy, in addition to the usual approvals required to conduct such activity (e.g. under a valid warrant).

## *Records*

Any indication or assessment of an individual's status as a sensitive category individual should be recorded, along with the basis for the assessment. This documentation should be made available for internal audit purposes on request.

The policy sets out a range of approval processes and procedures for each category of sensitive individual.

## **Policy in respect of children and young persons**

All children and young persons are considered to be sensitive category individuals, regardless of whether they are New Zealanders or not.

Personal information of children or young persons may sometimes be collected inadvertently through the identification of close relatives. Staff should take all feasible and practicable measures to protect the private identifying details of children and young persons from dissemination outside the agencies unless directly relevant to the organisation's functions and approved for release through the relevant authority.

The Ministerial Policy Statement on "Collecting information lawfully from persons..." provides that NZSIS will not seek to use children and young people as human sources.

Any investigation, operational, or collection activity involving a child or young must be authorized by an appropriate authority in accordance with internal policy.

Staff authorized to conduct interviews must ensure that a support person is present at any interview with a child or young person.

## **Policy in respect of people vulnerable by reason of illness or other capacity**

All people vulnerable by reason of illness or other incapacity are considered to be sensitive category individuals, regardless of whether they are New Zealanders or not.

Where it is unclear if a person is vulnerable for such a reason, advice should be sought internally or externally, as operational security permits.

Any investigation, operational, or collection activity involving a person vulnerable by reasons of illness or other capacity must be authorized by an appropriate authority in accordance with internal policy.

## **Policy in respect of New Zealand Members of Parliament (MP)**

Further information about NZSIS investigative activities impacting on MPs can be found in the Memorandum of Understanding between the NZSIS, the Minister responsible for NZSIS, and the Speaker of the House.

In circumstances where GCSB or NZSIS determine it is necessary to carry out investigative or operational activity where the subject is a New Zealand MP they must seek approval from the Director-General.

GCSB or NZSIS must ensure appropriate conditions or restrictions are in place to minimise collection of information protected by parliamentary privilege.

If it becomes necessary to obtain an authorization against a sitting MP, a classified briefing must be provided to the Speaker of the House. The Director-General must consider, in consultation with the Speaker, whether any restrictions or conditions should apply to the authorization to minimize any impacts on proceedings in Parliament.



## **Policy in respect of members of the New Zealand judiciary**

If a staff member considers it necessary to carry out any investigative or operational activity involving a current member of the New Zealand judiciary, approval must be obtained from the Director-General, who may wish to provide a briefing to the Chief Justice.

## **Policy in respect of journalists**

All journalists are considered to be sensitive category individuals, regardless of whether they are New Zealanders or not.

Any investigative and operational activity about or directly involving a journalist increases the risk that the agency could be perceived to be interfering with the freedom of expression and the protections afforded to journalists' informants. Such activity will require consideration of these risks, including steps to minimise collection of journalistic sources, where this is irrelevant to the investigation.

Determining whether or not a person is a journalist will depend on the circumstances, based on whether the person's normal course of work involves the preparation of news, and analysis of or commentary on news, for publication or broadcast in a public news medium.

A news medium includes, for example, a newspaper, magazine, news website or radio or television news programme. A blogger who regularly disseminates news to a significant body of the public can be a journalist, particularly if the blog publishes recent information of public interest. If there is doubt about whether a person is a journalist, legal advice must be sought.

### *Responsibilities of NZSIS staff*

Investigating a journalist may be required for the performance of NZSIS functions (e.g. if a journalist is obtaining classified material from an individual who holds a security clearance).

In such cases, staff need to be cautious when obtaining information that may reveal unrelated journalistic sources. Noting the confidential nature of journalistic sources, management approval must be obtained before commencing an investigation into a journalist and mitigations must be addressed.

Any collection activity, information assurance or cyber security services involving journalists must be approved by an appropriate authority in accordance with internal policy.

## **Policy in respect of claimants, refugees and protected persons**

GCSB and NZSIS have an obligation to protect information relating to the status of claimants, refugees and protected persons in accordance with the Immigration Act 2009 as well as the UN Refugee Convention, the Convention Against Torture and the Covenant on Civil and Political Rights.

The only circumstances in which GCSB or NZSIS may disclose the fact that a person is a claimant, refugee or protected person (whether they are being considered for status, have been considered in the past, hold a status, or previously held a status) are, in accordance with the Immigration Act (2009):

- a. For the purposes of determining the claim or matter, administering the Immigration Act or determining any obligations, requirements or entitlements of the claimant or other person concerned under any other enactment; or
- b. For the purposes of the maintenance of law, including for the prevention, investigation and detection of offences in New Zealand or elsewhere;

- c. To the United Nations High Commissioner for Refugees (or a representative of the High Commissioner)
- d. If the particulars relating to a claim are disclosed in a manner that is unlikely to allow identification of the person concerned;
- e. If, in the circumstances of the particular case, there is no serious possibility that the safety of the claimant or any other person would be endangered by the disclosure of the information; or
- f. If the individual has expressly waived his right to confidentiality; or by his or her words or actions, implicitly waived his or her right to confidentiality.

Any decision to share intelligence that identifies or has the potential to identify a person as being a refugee, claimant or protected person must be authorized by the appropriate authority in accordance with internal policy.

Sharing is only permitted for the performance of GCSB and NZSIS functions and must be carried out in accordance with all internal policy and procedures. GCSB and NZSIS should consider the inclusion of appropriate caveats to ensure the information is sufficiently protected.

# Summary: Sensitive Category Individuals Policy

*Policy approved 29 July 2021*

*Summary prepared under section 16(1)(e) of the OIA, in order to protect the interests of section 6(a).*

## Introduction

The legislative and compliance framework the NZSIS operates within requires the agency to have policies in place to ensure operational collection activity involving sensitive category individuals is appropriately authorised and managed.

The relevant policy outlines the types of individuals and situations the agency considers sensitive and sets out GCSB and NZSIS's obligations towards these individuals. Their information, and privileged information as required by the Intelligence and Security Act 2017 and Ministerial Policy Statements.

## Policy

### *Scope*

The policy applies to all GCSB and NZSIS staff, and any person currently working under the authority of or engaged by GCSB or NZSIS.

The policy applies to situations where the subject of the information or activity is a sensitive category individual, or where a sensitive category individual is not the subject but may be indirectly affected by agency activities, or where the activity involves access to privileged information.

### *Defining a Sensitive Category Individual*

The policy establishes three categories of SCIs:

- Sensitive because they are vulnerable

- Sensitive because of their access to New Zealander's privileged information

- Sensitive because of their occupation/role

### *Assessing whether a person is a Sensitive Category Individual*

Staff must be alert to any factors that may increase the likelihood of encountering a sensitive category individual or their data, as sometimes staff will not know they are interacting with a person in this category.

Reasonable efforts using already available information must be made to determine if investigative or operational activity is being conducted about, or directly involves, a sensitive category individual. Staff must not however, undertake further intrusive activity for the sole purpose of making that assessment.

### ***Sensitive because they are vulnerable***

Children and young persons: a child means a person under 14 years. A young person means a person aged 14 or over and under 18. This policy applies to New Zealand and foreign children and young people.

Staff must seek to confirm a date of birth to determine if an individual is a child or young person. If there is any indication that an individual is a child or young person then they should be considered a child or young person until confirmation can be obtained.

#### *Persons vulnerable by reason of illness or other incapacity*

This policy applies to New Zealand and foreign persons vulnerable by reason of illness or other incapacity.

Where it is unclear if a person is vulnerable for such a reason, advice should be sought internally or externally, as operational security permits.

#### *Refugees, asylum seekers, claimants and protected persons*

This policy applies to New Zealand and foreign refugees, asylum seekers, claimants and protected person. To be considered a refugee, asylum seeker, claimant or protected person, the individual must fall within the definitions outlined in the Immigration Act 2009; with reference to the UN Refugee Convention, the Convention Against Torture, and the Covenant on Civil and Political Rights.

#### ***Sensitive because of their access to New Zealanders' privileged information***

Privilege is protected by law. It recognizes public interest in protecting certain New Zealanders' communications or information in the context of particular relationships.

Under the ISA, privilege holders can only be New Zealand citizens or those holding a New Zealand permanent resident visa. The policy also applies to overseas individuals who have privileged communications with New Zealanders to ensure the protection of the privileged information of the New Zealander.

#### *Lawyers/legal advisors*

It may be difficult to determine whether an individual is a legal advisor before beginning activity. Staff must consult with the relevant agency's legal team if in doubt.

#### *Medical practitioners*

A medical practitioner is a health practitioner who is registered with the Medical Council of New Zealand as a practitioner of the profession of medicine. AS a matter of policy, the agencies also consider medical practitioners registered to equivalent bodies overseas who are consulted by New Zealanders to be SCIs in the same way as medical practitioners registered in New Zealand.

#### *Minister of religion*

Whether a person is a minister of religion will depend on their status within a church or other religious or spiritual community. This policy applies to New Zealand ministers of religion, and foreign ministers of religion who are consulted by a New Zealander.

If there is any doubt about whether a person is a minister of religion, staff must seek advice from the relevant agency's Compliance or Legal team.

#### ***Sensitive because of their occupation/role***

##### *New Zealand Members of Parliament (MPs)*

Staff are expected to confirm whether an individual is a Member of New Zealand's Parliament through open source checks.

### *Members of the Judiciary*

Staff are expected to confirm whether an individual is a member of the New Zealand judiciary through open source checks.

### *Journalists*

A journalist is an individual whose normal course of work involves the preparation of news, and analysis of or commentary on news, for publication or broadcast in a public news medium, and who is a New Zealander, or employed as a journalist in New Zealand or by a New Zealand media company.

If there is any doubt about whether a person is a journalist, staff must seek advice from the relevant agency's Compliance or Legal teams.

## **Policy Principles**

### *All activity must be lawful, necessary, and proportionate*

The fact that a person is an SCI does not prevent agencies conducting activity involving the person or their information however staff and relevant approvers must ensure that any activity involving an SCI is lawful, necessary and proportionate.

*Staff must act in accordance with this policy when conducting any activity involving or likely to involve Sensitive Category Individuals, their information, or privileged information.*

Staff must be alert to any factors indicating the presence of an SCI or that may increase the likelihood of encountering an SCI or their data, and apply this policy when it is likely that the activity involves an SCI or their information.

### *Identifying SCIs*

Staff must consider all available information to determine if investigative or operational activity is being conducted about, or directly involves, a sensitive category individual. If so, staff must seek approval at the required level according to the policy.

If a person is identified as a sensitive category individual after collection, the continuation of the activity or the use of the information must be approved in accordance with this policy. If the information is irrelevant, it should be destroyed.

### *Approval levels*

The policy establishes a regime that must be followed for authorising any investigative or operational activity against sensitive category individuals. Staff must ensure that any activity involving a sensitive category individual is appropriately authorised using the framework established in the policy, in addition to the usual approvals required to conduct such activity (e.g. under a valid warrant).

### *Agency documentation and record keeping*

The agencies will ensure that requirements regarding SCI's information and privileged information are clearly recorded in all relevant internal guidance.

## **Extract from GCSB NZSIS Joint Policy Statement: Obtaining and using publicly available information**

### *Copyright considerations*

34. The majority of GCSB and NZSIS's collection of open source information will not result in a copyright infringement. Where it does, it may be provided for under the statutory exemption contained at section 63 of the Copyright Act 1994; where copyrighted material can be used by or on behalf of the Crown for the purpose of national security.
35. Where GCSB or NZSIS employees have any concerns or uncertainty as to whether actions or proposed actions have, or will result, in a copyright infringement they should seek advice from the relevant legal team.