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[1], can be carried out on an ordinarily lawful basis without an intelligence warrant or authorisation under section 78 of the Act.

This 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;

[1] *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:

   e) 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 (*Section 121 requests MPS*);

      iii. by collecting, requesting and receiving information from a person (known as human intelligence activities) (this MPS);

      iv. from overseas public authorities (*Cooperating with overseas public authorities* MPS);

   f) Obtaining, collecting and using publicly available information (*Publicly available information MPS*);

   g) Through the conduct of other lawful activities, such as conducting surveillance in a public place (*Conducting surveillance in a public place MPS*).

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*;
    - 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*;
    - 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.*

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;*

- 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, *Information assurance and cybersecurity activities*;
- 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.[2]
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 must have systems in place to support and monitor compliance. These policies and procedures must also address the following matters:

Procedural fairness

28. 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.
29. 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

---

[2] *This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.*

Representations

30. 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* and *Assumed identities*). 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.
31. 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

32. 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).
33. 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.
34. Internal policies should require legal advice and any other advice to be sought where appropriate.

Remuneration

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

Conflicts of interest

36. 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.
37. 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

38. GCSB and NZSIS must have a policy setting out the restrictions and protections necessary in the conduct of activities in respect of sensitive categories of individuals (for example, children and young people aged under 18 years of age, people vulnerable by reason of illness or other incapacity, refugees and asylum seekers, New Zealand Members of Parliament, members of the New Zealand Judiciary and journalists).

39. 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.
40. 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

41. 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

42. 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

43. 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

44. 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.
45. 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 and/or GCSB and MFAT in respect of such activities and the MPS on *Cooperating with overseas public authorities.*

Cooperation with and assistance from other agencies

46. 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.

47. 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.

48. 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

49. 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

50. GCSB and NZSIS are subject to 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

51. 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.

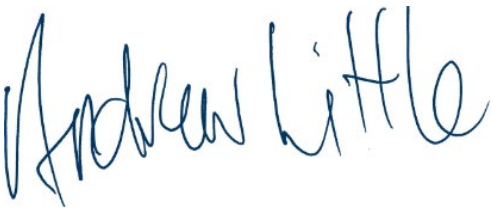
52. The identification and management of operational, reputational, legal, and health and safety risks should be carried out in accordance with a risk management policy.

53. The Directors-General of the GCSB and NZSIS should have delegations in place for such authorisations.

Duration of Ministerial Policy Statement

54. This MPS will take effect from 01 March 2022 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
01 March 2022