Ministerial Policy Statement

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

Summary

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

Definitions

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

GCSB *means the Government Communications Security Bureau.*

NZSIS *means the New Zealand Security Intelligence Service.*

Purpose

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

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

3. MPSs are also relevant to oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of her propriety jurisdiction (the Act requires the Inspector-General of Intelligence and Security to take account of any relevant MPS and the extent to which an agency has had regard to it when conducting any inquiry or review).

4. Every employee making decisions or taking any action relating to collecting information lawfully from persons within the scope of this MPS must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General are responsible for ensuring the MPS is reflected in their agency's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

Scope

5. This MPS applies to the collection of information lawfully from persons without an intelligence warrant or authorisation given under section 78 of the Act. It is intended to cover lawful human intelligence activities (or 'HUMINT'). Human intelligence is obtained from people with knowledge of or access to information. Human intelligence may come from a range of sources – from covert human intelligence sources at one end of the spectrum, to private individuals who independently offer information, at the other end. This means human intelligence activities include a broad array of activities, from working with covert human sources and protecting them by helping them conceal their involvement with GCSB and NZSIS, through to engaging openly with community members or interested members of the public.

6. This MPS applies regardless of whether information is collected from a person in a face-to-face meeting, over the Internet, or via any other form of communication. Where information is collected through the use of an assumed identity this MPS should be read in conjunction with the MPS on *Acquiring, using, and maintaining an assumed identity*.

7. The agencies regularly request information from other organisations and individuals in the performance of their functions (for example, they may approach a business to confirm address details through billing records). These requests are always made overtly; that is, it is clear that the requester is from an intelligence and security agency. This MPS does not cover those types of information gathering activities, which are covered by a separate MPS (see MPS on *Requesting information from agencies under section 121*).

8. Nor does this MPS cover the creation, maintenance, and use of assumed identities or corporate identities for the purpose of undertaking intelligence collection or other activities, false and misleading representations relating to employment with an intelligence and security agency (that is, personal cover), or open source intelligence collection. Those activities are covered by separate MPSs (see *Making false or misleading representations under section 228 about being employed with an intelligence and security agency* and *Obtaining and using publicly available information*).

9. This MPS only relates to ordinarily lawful human intelligence activities; it does not therefore cover unlawful human intelligence activities that may only be carried out under an

authorisation. Such activities must be conducted in accordance with the terms of that authorisation, including any restrictions or conditions set out in the authorisation.

Context

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

Principles

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

Legality

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

Necessity

25. Human intelligence activities should only be carried out when necessary to enable GCSB or NZSIS to perform their statutory functions. Those activities – including those needed for security, training, or the development of capabilities – should be directed towards the performance of those functions. In some circumstances, it may be necessary for GCSB or NZSIS to collect similar or the same information from a range of different persons – for example, where GCSB or NZSIS need to obtain the information from a number of sources in order to assess the reliability of the information.
26. This reflects the law in relation to the collection of personal information – information privacy principle 1 of the Privacy Act 1993 provides that personal information should not be collected unless the information is being collected for a lawful purpose connected with a function or activity of the agency and the collection of the information is necessary for that purpose.

Proportionality

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

Less intrusive means to be considered

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

Minimal impact on third parties

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

Oversight

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

Matters to be reflected in internal policies and procedures

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

Appropriate conduct, including compliance with the State Services Code of Conduct
The Directors-General of GCSB and NZSIS must issue policies and procedures that reflect the agencies' obligations under the State Sector Act 1988.

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

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

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

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

Sensitive category individuals
GCSB and NZSIS must have a policy setting out the restrictions and protections necessary in the conduct of activities in respect of sensitive categories of individuals (for example, children and young people aged under 18 years of age, Members of New Zealand's Parliament, members of the New Zealand judiciary, journalists, lawyers, registered medical practitioners or other providers of health services attracting medical privilege, and people vulnerable by reason of illness or other incapacity).

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

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

Health and safety

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

Training

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

Use of information collected from human intelligence activities

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

Human intelligence activities undertaken overseas

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

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

Cooperation with and assistance from other agencies

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

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

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

Representations

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

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

Information management

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

Compliance with the information privacy principles

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

Authorisation procedures

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

Duration of ministerial policy statement

35. This MPS will take effect from 28 September 2017 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 Christopher Finlayson
Minister responsible for the Government Communications Security Service
Minister in charge of the New Zealand Security Intelligence Service

September 2017