POLICY ON THE RELEASE OF INFORMATION

Preamble and Scope

This policy is to guide decision making on responding to information requests under the Privacy Act and Official Information Act.

Typically such requests relate to individuals or to organisations and this policy is directed to these information requests. Requests for corporate information are not specifically covered by this policy. In some cases individuals will be 'in record' as they have a vetting file or were a referee and this policy does apply to these requests.

This policy should be read in conjunction with the Service's *NZSIS Information Management: Archives Policy (available on the intranet).*

Objective

The purpose of this policy is to ensure that NZSIS:

- responds appropriately to information requests
- protects specific areas of investigation (with the corollary that we may not disclose areas that are not of interest)
- protects sensitive sources or methods
- protects the identity of NZSIS staff.

This will enable NZSIS to fulfil its responsibility to provide access to information and ensure it maintains its ability to operate effectively as an intelligence organisation.

Context

In considering information requests to the NZSIS the unique characteristics of the NZSIS's business need to be taken into account including:

- the long term nature of Service investigations
- the Service's investigations are necessarily prospective in nature
- at some point individuals and organisations that were of security interest may cease to be of interest. The fact that they were of security interest may also cease to be a matter requiring protection from disclosure

- subjects of Service investigation are often adept at concealing their activities
- the Service is a natural target for strategic/orchestrated requests
- reputation of being willing and able to keep confidences is of paramount importance
- the Service's relationships with agencies of the governments of other countries need to be preserved
- disclosing could have repercussions on the .

Any compromise of necessary confidentiality would inevitably impact on the operational effectiveness of the Service in fulfilling its security functions and would be likely to prejudice security.

Starting with this context, a system for reliably assessing the sensitivity of information is required.

Assessing Information Requests

There is no simple formula or rule that can be applied to decide whether or not to release information. The following framework is intended to provide a guide to assist in the process.

Categories of information

The Service's experience in dealing with information requests is that its holdings generally fall into one of three categories.

CATEGORY 1: Inherently sensitive – withholding grounds likely to apply
CATEGORY 2: Not inherently sensitive – withholding grounds may apply
CATEGORY 3: No information held – withholding grounds likely to apply to protect inherently sensitive information from orchestrated requests and disclosure of what the Service doesn't know.

CATEGORY 1: Inherently sensitive information

If there is inherently sensitive material, then its very existence is also likely to be sensitive. Sensitivity inevitably relates to the need to keep the information secret to preserve its effectiveness in the national security context. In some circumstances the information itself may not appear sensitive, the fact that the Service holds it makes its existence sensitive.

Specific areas of investigation

- Disclosing the existence of an investigation, particularly if it is recent or current, would cause the subjects of the investigation to alter their behaviour so as to conceal their activities, frustrating investigation techniques.

- The sensitivity of a Service investigation can have a long life, as the Service is often dealing with threats posed over lengthy periods by subjects who are thinking and planning long-term.

- We cannot presume any length of time will automatically ease security concerns. It depends on the subject matter, and sensitivity should be considered at the time the request is made. That said at some point individuals and organisations that were of security interest may cease to be of interest and the fact that that they were of security interest will also cease to be a matter requiring protection from disclosure.

- We also need to consider the New Zealand context:

    - Small communities:
        - the small size of communities, including those of immigrant populations whose members may be facilitating activities overseas, means most will know each other; unexpected, future changes in circumstances of country of origin may renew Service interest in a group;
        - those involved in (or on the periphery of) New Zealand groups that tend toward violent protest or worse, know each other fairly intimately and this seems to carry across generations;

    - Revealing a past investigation affecting a particular community or group is likely to reveal existence of sources, or arouse suspicions of source reporting where none existed. It may also disclose methods still used. Methods may not be generally known, even if they have carried on for tens of years (eg extent of liaison/government sharing, use of sources etc)

    - Because of the transnational activity of those involved in WMD activity, revealing a specific investigation would reveal methods (and place) of detection;

    - Safety, trust and confidence of sources (including liaison) will not diminish with the passage of time. Even with redaction, revealing an area of investigation could point to a source given the small size of communities in New Zealand.

Prospective nature of investigations

The Service must be forward-looking to anticipate threats to the State. This means the Service needs to preserve its position as to whether material may be relevant in the future although its relevance is not currently obvious.

Sensitive sources

Disclosing any information that would lead to the disclosure of the existence of a source would affect the particular individual's safety and would also be contrary to the public interest, because it would likely impact on all sources' expectations of confidence in dealing with the Service.

Sensitive methods

A method of collecting information may be sensitive in or of itself, because it is not generally known to exist, or the extent of its use or effectiveness is not generally known. Or, the method itself may not be sensitive but its use in a particular operation is.

Revealing a past investigation may also disclose methods still used. Methods may not be generally known, even if they have carried on for tens of years (eg etc).

Sensitive methods include the Service's .

Liaison

Information shared with New Zealand by the government of another country or its agency cannot be released if that government or agency, known here as "liaison partner", as the owner of the material, does not consent to its release. This same principle applies to New Zealand information shared with other countries.

Privacy of others

The Service should not provide information about others. Care must be taken to protect the privacy of others when releasing information.

CATEGORY 2: Information that is not inherently sensitive

General areas of interest to the Service

References to general areas of investigation or interest are not sensitive if they have been disclosed, eg in the unclassified annual report or on the Service's website.

General processes for obtaining information

Disclosing general information about how information is obtained, for example the fact that sources or some methods are used is not likely to prejudice security (eg interviewing, interception, telecommunications data, covert surveillance).

Prior knowledge of Service holding

The fact that the Service holds information about a person or subject will not be sensitive where the existence of the Service's holding is already known publicly or to the individual. This can include:

- *Legal processes*
- *Person initiated contact with Service:* individual initiated contact with the Service, either to offer information, or as a "correspondent of unconventional perceptions" (or both).

- *Vetting:* the Service holds information about a person because they have been vetted for a security clearance or been a vetting referee.

- *Service disclosed an interest:* in some cases, the Service may have already disclosed that it holds material on a person or subject area. In such cases there is no sensitivity about the fact that the Service holds information about them.

Outdated methods

A method that is no longer used or is already sufficiently public may not be sensitive, depending on the particular circumstances.

Liaison material

Liaison partners may decide to agree to the release of material because they do not consider the material sensitive – eg because of the passage of time or a legal process makes the existence of the material public (eg).

CATEGORY 3: No information

The sensitivity of simply advising the non-existence of information is:

- it discloses what the Service does not know

- it leaves the Service open to orchestrated requests designed to identify specific areas of investigation.

Both impact on CATEGORY 1 information, ie information which is inherently sensitive.

The consequences are:

- the deterrent effect of not knowing whether or not the Service is investigating a particular activity is lost

- telling a person they have not been detected leaves them free to carry on or escalate their activities.

The Service is a natural target for orchestrated requests by some persons of security concern who want to understand more about the Service's specific areas of investigation.

Because the Service has no way of knowing who is making a bona fide request and who is not, it must apply the neither confirm nor deny response to protect its specific areas of investigation.

On this basis, requesters for whom no information is held under their name or subject should be issued with a response that neither confirms nor denies the existence of information.

Overview of the Process for Responding to Information Requests

When an information request is received, the following process is applied:

- Check whether any information relevant to the request is held.

- If yes, consider whether the existence of the material is inherently sensitive in itself because it discloses a specific area of investigation; the use of a sensitive source or method; or use of liaison reporting. Consider the holdings about the person or subject as a whole (not a detailed consideration of every record).

- If the existence of the Service's holdings is not inherently sensitive, the relevant records must be assessed individually as to whether they are:

    - inherently sensitive; or
    - not inherently sensitive.

At this point, any decision to release will be made only where there is no likely prejudice to security or to a person's privacy. (Likely to cover only material that is not inherently sensitive.)

- If no information is held, the non-existence of the information is inherently sensitive, as it discloses what the Service is *not* investigating. It will be necessary to neither confirm nor deny the existence of information to protect the Service from orchestrated requests and disclosing "what it doesn't know". Exceptions can be made where:

    - If the information *did* exist, it would not be likely to prejudice security (eg because the Service knows the correspondent or they are elderly).

    - It is important for the safety and wellbeing of the individual that the Service confirms no information is held.

    - There is a significant overriding public interest issue.

Signed:

Warren Tucker (D)

Date:

Responsibilities

Action	Description	Role
Approve Policy	Approval of Policy, processes and responsibilities	Director/
Review Policy	Monitor effectiveness of the Policy and recommend changes/improvements	
Develop and maintain processes	Processes must support the effective and efficient implementation of the policy	
Receipt and processing of Information Requests	Receipting and acknowledging information request, assessing information holdings and preparing responses	Archives Section
Review responses for security	Review proposed responses to ensure areas of investigation, sources and methods are not compromised	(or delegate)
Advise on the Privacy Act and OIA	Advise on the interpretation application of the Privacy Act and OIA	
Respond to the Privacy Commissioner/Ombudsman on complaints	Liaise with the Privacy Commissioner/Ombudsman when they are investigating complaints about NZSIS responses to Information Requests	Director/
Assist Privacy Commissioner/Ombudsman investigating complaints	Provide access for Privacy Commissioner/Ombudsman to information holdings when they are investigating a complaint	Archives Section
Respond to media	Release of information may draw media attention and questions directed to the Service	

Principles and Guidelines for Dealing with Statutory Access Regime Requests

Background

Since the passing of the Official Information Act 1982 (OIA) and the Privacy Act 1993, the Service has gradually evolved a set of precedents that is applied when responding to requests made under this legislation. Although cognisance is taken of the Service archives policy, which was promulgated in August 2003 and continues to evolve, the archives policy is specifically excluded from directing the Service's response to requests for information made under the statutory access regimes.

With a steady increase foreseen in requests made under the OIA and the Privacy Act, it is desirable to standardise the way in which such requests are dealt with. This will help ensure consistency of decision-making, enable extra staff to be more easily be deployed to respond to requests, and help ensure that statutory response times continues to be met.

The purpose of this paper is to codify current practice for handling requests for information made under the OIA and the Privacy Act. The points are arranged in order of importance. Thus, there is a presumption that information will be released, subject to the interests of the Service, notably security, being met.

Principles and Guidelines

- Information will be released where this does not conflict with Service interests.

The range and volume of archival material being released is increasing, but information will continue to be withheld where it is in the interests of the Service to do so. This will usually be for security and privacy reasons. On rare occasions it may be necessary to release information that would normally be regarded as sensitive. For example, the Service might wish to provide information where a person had voluntarily and deliberately revealed their association with the Service and consequently been the subject of publicity, or had requested that the relationship be revealed.

- Security is of paramount concern.

The preservation of security is a core contributor to the business effectiveness of the organisation and its mission; and the NZSIS therefore has an obligation, of high order in its priorities, appropriately to protect:
- the identities of individuals who work for or assist the work of the Service, and the nature of that work and assistance;
- sensitive techniques whose disclosure could endanger national security; and
- information proffered by or solicited from third parties such as partner agencies inside and outside New Zealand whose unauthorised disclosure could imperil those relationships.
The maintenance of national security will be a key test in making judgements on requests.

- Due regard must be had for privacy.

Private citizens are entitled to greater privacy than public figures, and sensitive information will not generally be released unless the subject consents, the information is

already in the public arena, or an appropriate period has passed. Information about criminal convictions, health, and family circumstances such as adoption, for example, will be withheld during the lifetime of the individual, and perhaps that of their children, but there is no obligation to withhold records of political excesses, even when it was the product of youth. That said, some particularly egregious activity (for example violence or spying) may call for more careful consideration of all the circumstances. Time will diminish privacy concerns. The Service will be guided by relevant legislation and practice.

- Where there is a high level of public interest privacy issues, but not security issues, may be outweighed and the information released or the withholding period reduced.

- The security significance and context of the record must be taken into account.

Considerations include the nature of the person's activity, their allegiance (for example a New Zealand citizen furthering foreign interests inimical to those of our nation), and historical context. For example, past involvement in public protests is often considered a badge of honour, whereas spying for a foreign power is still seen as perfidious. There is a popular view that traitors should not be shielded but they and their families should have some rights – for example, to preview material being released and put their side of the story.

- Broader Service policy objectives are an appropriate consideration when deciding whether or not to release information.

It is legitimate to release information to further a Service policy of, for example, moving towards greater openness or raising the public profile.

- The volume of material and nature of the processing required are valid considerations when deciding whether or not to release information.

The OIA provides that the request may be refused if the information cannot be made available without substantial collation or research; the Privacy Act has a similar provision if the information is not readily retrievable.

- Each request will be assessed on an individual basis.

Requests for information will be treated as having been made under the Official Information Act 1982 (OIA) and the Privacy Act 1993, as appropriate, whether or not the applicant refers to the relevant Act. Each request will be assessed on an individual basis and the Service will act in the spirit of these statutes, while taking full account of security and privacy considerations. The Service archives policy does not provide guidance on responding to requests made under these Acts . However, where appropriate, cognisance may be taken of the evolving archives policy and practice.

- The use of the "neither confirm nor deny" provision will be appropriate in some circumstances.

Although use of the "neither confirm nor deny" provision has been criticised by the Chief Ombudsman and the Privacy Commissioner, it will be the appropriate response when for

example a person poses a significant current threat to security, or is party to an orchestrated plan to collect and analyse intelligence.

- Information will not be withheld just because it reflects badly on the Service.
- Access decisions, especially for older records, will be subject to periodic review.
- Material being declassified will be made available to all interested parties

A register is kept of those who have indicated an interest in the subject, and they will be provided with copies of relevant material as it becomes available - except that some personal information may be releasable only to the person, or the close family of the person, who is in record.

- Where possible the Service will process material requested by members of the public, and, as resources permit, other records judged to be of the most interest to the public. Private requests which involve substantial research or processing will not be given precedence, however.
- Where the information that is releasable is not representative of Service holdings and would create a false impression, it will be issued with a clarificatory statement. If this is not possible, the information may be withheld.
- Where a correspondent with unconventional perceptions has concerns which might be allayed by a response from the Service, every endeavour will be made to meet their request.
- In exceptional cases, privileged access may be granted.

Supervised access to selected archives at NZSIS Headquarters may be granted on a case-by-case basis as negotiated (usually only with official historians).

Process

Responsibility for managing requests for information made under the statutory access regimes will rest with [redacted] Requests received will be scanned by Registry staff and forwarded to [redacted] Section. [redacted] staff will maintain an electronic register of requests which will be sent to DDC monthly. [redacted] staff will consider each request and recommend to DDC the appropriate response. DDC will decide the response, or refer the decision to the Director.

[redacted] staff will ensure that all material to be released is expurgated of any references that might compromise security and is formally declassified. When deletions are necessary, the release copy will be annotated to indicate where and why this action has been taken, and the recipient advised of his or her right of appeal.

It is the responsibility of [redacted] staff to ensure that original records are kept intact, and that an accurate record is kept of all documents released, including any deletions or excisions made.

Classification: UNCLASSIFIED

Application of s10 of the Official Information Act 1982 and s32 of the Privacy Act 1993 by the NZSIS

INTRODUCTION

1. The success of the investigatory work of the NZSIS relies on discretion and the keeping of confidences. The general principle of neither confirming nor denying the existence or non-existence of information, particularly in relation to investigatory-type information, allows that work to continue.
2. This document sets out the circumstances in which the "neither confirm nor deny the existence of information" response is applied to requests for information made under either the Official Information Act or the Privacy Act.
3. The NZSIS often relies on the "neither confirm nor deny" response, and this document aims to explain the reasons for that response.
4. The NZSIS is also concerned that individuals who are the recipient of a neither confirm nor deny response should understand that this does not mean they are necessarily of security interest. Usually, they will be of no concern to the NZSIS at all. But the unique nature of the NZSIS work means it must neither confirm nor deny the existence of information broadly, in order to preserve its investigatory work.

INFORMATION THAT CAN BE DISCLOSED

5. The NZSIS has a number of roles prescribed by the NZSIS Act. Across many of these activities the NZSIS tries to be open about its general areas of interest, is able to disclose the existence of information, and is able to release certain files (subject to the requirements of the Official Information Act, Privacy Act and NZSIS Act). These include:

   - *Legal processes:* Where an individual knows the NZSIS has information as a result of legal processes, the fact of the NZSIS's holdings is not sensitive. Examples of this are the Zaoui and Sutch cases.
   - *Person initiated contact with NZSIS:* Sometimes, the sole reason the NZSIS has information on its files relating to an individual, is because the individual initiated contact with the NZSIS, either to offer information, or for other reasons.
   - *Vetting:* The NZSIS may hold information about a person because they have sought a security clearance or been a referee for a person seeking a security clearance, a process that falls within one of the functions of the NZSIS. The fact of this holding is not sensitive.
   - *NZSIS disclosed an interest:* For whatever reason, the NZSIS may have already disclosed that it holds material on a person or subject area. In such cases there is no sensitivity about the fact that the NZSIS holds information about them.

SECURITY INVESTIGATIONS ARE SENSITIVE

6. The core function of the NZSIS is:

   > "To obtain, correlate, and evaluate intelligence relevant to security, and communicate any such intelligence to such persons, and in such manner, as the Director considers to be in the interests of security."

7. The work of the NZSIS protects national security and advances New Zealand's interests. Such work includes:

   - Safeguarding New Zealand from the actions of foreign powers that might otherwise damage the interests of New Zealand.
   - Preventing the potential facilitation of terrorists acts both in New Zealand and overseas.
   - Preventing the spread of weapons of mass destruction.

8. The NZSIS operates in a unique environment, which poses particular challenges for investigatory work.
9. Security investigations are long-term in nature. Partly, this is related to the nature of its subjects, many of whom think and plan long-term. Often, they have undertaken specialist training to learn how to conceal their activities. It can require long lead time on the part of the NZSIS to gain access to information about such subjects.
10. Security intelligence investigations also have a longer life than law enforcement investigations. The latter are typically brought to a close by the laying of charges. But that is not the case for the NZSIS which is not an enforcement authority. For the NZSIS, the closing of an investigation does not mean that the investigation is no longer sensitive.

11. NZSIS investigations are also prospective in nature, with the primary emphasis on prevention. The NZSIS will often need to preserve its position as to whether material may be relevant in the future.

12. The NZSIS collects intelligence from human sources and by visual and technical surveillance. These sources and methods are used covertly so as not to reveal investigations and to allow the NZSIS to access intelligence that would not otherwise be available.

DISCLOSURE CAN PREJUDICE SECURITY

13. In some cases, general areas of investigation can be disclosed in the unclassified website. However, in the case of specific investigations, both collection methods and investigative effectiveness would be compromised if the subjects of investigation knew when and how such techniques were being deployed.

14. Effectively, a request for information to the NZSIS is tantamount to asking whether there is or has been an investigation by the NZSIS into the individual or the subject matter. The NZSIS is particularly susceptible to orchestrated requests by people who are seeking to know whether they are under investigation.

15. As well as protecting security investigations, the NZSIS needs to protect its reputation and its ability to keep confidences. Disclosing information that would lead to the disclosure of the existence of a source would affect people's safety and be contrary to the public interest, because it would likely impact on all sources' expectations of confidence in dealing with the NZSIS.

16. Security concerns about individuals or subjects may lessen over time, but not in all cases. At best, the passage of time will be relevant as to reduced sensitivity, but ultimately a judgement needs to be made about sensitivity (in terms of prejudice to security) and the likely consequences of disclosure at the time the request is made.

THE PROBLEM WITH CONFIRMING THAT NO INFORMATION IS HELD

17. It would seem straightforward that if no information is held, a reply confirming the non-existence of information could be provided without fear of likely prejudice to security.

18. Unfortunately, such an approach would be likely to prejudice security as:

- It discloses what the NZSIS does not know.
- It leaves the NZSIS open to orchestrated requests designed to flush out specific areas of investigation.

19. There are two principal concerns associated with confirming that no information is held:

- Not knowing whether the NZSIS is investigating a particular activity or not has something of a deterrent effect. If it becomes a simple exercise to identify what is not of interest to the NZSIS, the benefit of the deterrent effect is lost.
- If a correspondent is undertaking activities of security concern, and receives a "no information held" response for a subject they believed should be under investigation, they now know they have not been detected.

20. Unfortunately, the NZSIS is a natural target for orchestrated requests by some persons of security concern or their associates who want to understand more about the NZSIS' specific areas of investigation.

21. The only way to ensure that there is no prejudice to security is to be consistent in responses between these two groups (i.e. subjects of interest and subjects of no interest), and to issue a neither confirm nor deny response for both.

LEGAL PROTECTIONS

22. New Zealand legislation anticipates that special protection will be given to NZSIS information, including:

- Section 12A of the NZSIS Act which prevents any officer or employee of the NZSIS from disclosing any information obtained through their connection with the NZSIS otherwise than in the strict course of official duties or as authorised by the Minister.
- Section 13A of the NZSIS Act which makes it an offence for any person to publish or broadcast the fact that any person is a member of the NZSIS (other than the Director), or is connected in any way with a member of the NZSIS.
- Section 26 of the Inspector-General of Intelligence and Security Act 1996 which prevents the Inspector-General or any of his staff from disclosing to any person security records or other official information relating to the activities of an intelligence and security agency.

SAFEGUARDS AND OVERSIGHT

23. The reliance on the "neither confirm nor deny" response may cause concerns about whether the rights of individuals are being protected. However, the NZSIS is subject to a number of safeguards and oversight arrangements. They are:

Oversight by the Inspector-General of Intelligence and Security

- The Inspector-General, who must have held high judicial office, undertakes an annual review programme covering warrants and other statutory processes of the NZSIS.
- The Inspector-General can hear complaints under the terms of his Act.
- The Inspector-General can initiate a review of any NZSIS activity on his/her own motion and is given access to all NZSIS material.

Review by the Privacy Commissioner

- The Privacy Act 1993 allows the Privacy Commissioner to hear complaints on neither confirm nor deny responses or the withholding of information.
- The Privacy Commissioner's office reviews NZSIS files that are the subject of complaints.
- The NZSIS provides the Privacy Commissioner with access to all material that may be relevant.

Review by the Ombudsmen

- The Ombudsmen have jurisdiction to consider complaints about neither confirm nor deny responses or the withholding of information.
- The Ombudsmen review information held by the NZSIS.
- The NZSIS provides the Ombudsmen's Office with access to all material that may be relevant.

Political Oversight

- The Minister in Charge of the NZSIS is the Prime Minister, and the NZSIS must consult regularly with the Leader of the Opposition as well.
- The Intelligence and Security Committee - a body of politicians that has financial and policy oversight of the intelligence and security agencies - is made up of the Prime Minister, the Leader of the Opposition, two Members of Parliament nominated by the Prime Minister and one nominated by the Leader of the Opposition.
- The Director of the NZSIS must ensure that the NZSIS does not take action for the purpose of furthering or harming the interests of any political party.

Classification: UNCLASSIFIED

NZSIS Responds to Requests for Information

We have received many requests for information this year. The attached document explains how the NZSIS responds to these requests and why we frequently respond so that we can "neither confirm nor deny the existence of information".

The NZSIS protects national security and advances New Zealand's interests. Its work includes:

- Safeguarding New Zealand from the actions of foreign powers that might otherwise damage the interests of New Zealand
- Preventing the potential facilitation of terrorist acts both in New Zealand and overseas
- Preventing the spread of weapons of mass destruction

Across many of its activities, the NZSIS tries to be as open as possible. The NZSIS may be able to disclose the existence of information and release certain files, subject to the requirements of the Official Information Act, Privacy Act and NZSIS Act.

Examples where existence of information may be disclosed

- *Legal processes:* Where an individual knows the NZSIS has information as a result of legal processes, the fact of the NZSIS holdings is not sensitive. Examples of this are the Zaoui and Sutch cases.
- *Where the person initiated contact with NZSIS:* Sometimes, the sole reason the NZSIS has information on its files relating to an individual is because the individual initiated contact with the NZSIS, either to offer information, or for other reasons.
- *Vetting:* The NZSIS may hold information about a person because they have sought a security clearance or been a referee for a person seeking a security clearance, a process that falls within one of the functions of the NZSIS. The fact of this holding is not sensitive.
- *NZSIS disclosed an interest:* For whatever reason, the NZSIS may have already disclosed that it holds material on a person or subject area. In such cases there is no sensitivity about the fact that the NZSIS holds information about them.

Using Neither Confirm nor Deny Response

The NZSIS often relies on the "neither confirm nor deny" response to requests for information. The general principle of neither confirming nor denying the existence or non-existence of information, particularly in relation to investigations, allows our work to continue. The success of the investigatory work of the NZSIS relies on secrecy.

The attached document gives details for the "neither confirm nor deny" response and sets out the circumstances in which it is applied to requests for information made under either the Official Information Act or the Privacy Act.

If an individual receives a "neither confirm nor deny" response, this does not necessarily mean they are of security interest. Usually, they will be of no concern to the NZSIS at all. But the unique nature of our work means we must neither confirm nor deny the existence of information broadly, in order to preserve our investigatory work.

Investigations

The investigation tools used by the NZSIS include human sources and visual and technical surveillance, used covertly so as not to reveal investigations and to obtain intelligence not otherwise available.

Methods and investigation effectiveness would be compromised if the subjects of investigation knew when and how such techniques were being deployed. In particular the NZSIS is susceptible to group requests by people seeking to know whether they are under investigation.

It may appear that if no information is held on an individual or subject, the NZSIS could confirm the non-existence of information. Unfortunately, such an approach could prejudice security as it discloses what the NZSIS does not know, and also leaves the NZSIS open to orchestrated requests designed to flush out specific areas of investigation, or to identify the boundaries of our knowledge.

Legislation

New Zealand legislation offers special protection to NZSIS information – click here for details.

Safeguards and Oversight

The rights of individuals must be protected. The NZSIS is subject to several safeguards and oversight, including the:

- Privacy Commissioner,
- Office of the Ombudsmen,
- Inspector-General of Intelligence and Security,
- Intelligence and Security Committee,
- Commissioner of Security Warrants.