



COPY

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

THE HON D.P. NEAZOR CNZM

28 April 2010

Prime Minister

NZSIS RECORDS

Introduction:

1. Last year I reported to you on (i) the adequacy and suitability of the NZSIS policies relating to the creation, maintenance and closure of files on New Zealand persons in light of the Service's function under the New Zealand Security Intelligence Service Act 1969 and (ii) the adequacy and suitability of the Service's compliance with such policies in light of matters raised in the public domain (which centred on Members of Parliament).
2. You asked for a further short follow-up report on developments, which this is.

There are two central issues. The first was what the Service should do about people who have become members of Parliament in respect of:

- Any information held relating to them before their election;
- Any enquiry involving them after they become Members.

The second related to records in respect of other people.

The Parliament-related question

3. That has been dealt with in this way:
 - whatever files the Service had relating to Members of Parliament (by no means all Members), were closed and stored under the special control of one officer. Nothing is to be added while the person is a Member and no-one will be permitted access to such a file or data for the duration of the Member's Parliamentary term except to respond to Privacy Act requests. Any analogous electronic record is under similar control. After the Members' term ends, access will be permitted only on the Director's authority and when the Director is satisfied that to allow access would be consistent with his statutory obligations. How to deal with any existing references that may be in records not personal to the Member is still being worked on.

- the Director of Security has discussed with the Speaker of the House development of a formula which would reflect the conscience of the House and would state the circumstances in which it would be regarded as proper for the Service to collect and act on information about a person dealing with a Member, that other person being of security interest. A draft Memorandum of Understanding has been prepared and submitted to the Speaker for such consultation as he considers necessary.
- the arrangement just referred to would allow collection of information about a sitting M.P if that Member is suspected of undertaking activities detrimental to security. The collection would have to be personally authorized by the Director and before anything is done the Director would brief in confidence the Speaker of the House about the proposed collection, the reason for it and proposed action in the course of it. Parliamentary privilege would be protected.

The general part of the report:

4. I made two recommendations:

- that further consideration should be given to whether criteria can and should be developed to determine limits as to what is put into the Service's records.
- that attention should be paid to the periodic review of personal records whether held on paper or electronically, to determine whether the information held remains reasonably necessary for the Service's function, including reference and research, or whether information relating to a particular person should be destroyed or in effect closed and neither referred to nor added to unless there is some new justification for reviewing the matter. Reference was also made to the control of the use of any information passed to non NZ agencies with which the NZSIS has a working relationship.

5. After a further round of discussions with officers engaged in the assessment of information collected for intelligence purposes and with the operation of the Service's systems and controls, I have concluded that it is not useful to pursue those suggestions further because:

- tightening of collection practice covers the first and -
- resource demands and legal constraints make alternative approaches preferable to the second.

Relevant considerations:

6. There are a number of factors which bear upon the Service's record keeping:

- its statutory tasks;

- controls existing in the legislation governing the Service;
- internal controls related to collection, use and retention of information;
- changes in recording methods; and
- the nature of intelligence.

Statutory tasks:

7. Two of the Service's statutory tasks are:

- to obtain, correlate and evaluate intelligence relevant to security, and to communicate such intelligence to such persons and in such manner as the Director considers to be in the interests of security.
- to co-operate as far as is practicable and necessary, with such State Services and other public authorities in New Zealand and abroad as are capable of assisting the Service in the performance of its functions.

8. The reference to "security" is a controlling factor. The word is defined by law. Its broad ambit is the protection of New Zealand from acts of espionage, sabotage and subversion whether or not they are directed from or intended to be committed within New Zealand; the identification of foreign capabilities, intentions or activities that impact on New Zealand's international well-being or economic well-being; the protection of New Zealand from foreign activities that are clandestine or deceptive or threaten the safety of any person and impact adversely on New Zealand's international well-being or economic well-being; and the prevention of any terrorist act or related activity, not necessarily just in New Zealand.

9. That general control is supported by other legislative provisions which affect collection and record keeping.

Legislative controls governing the Service:

10. (i) as to collection:

- S 2(2) of the New Zealand Intelligence Service Act 1969 provides that nothing in the Act limits the right of persons to engage in lawful advocacy, protest, or dissent in respect of any matter, and, accordingly, that the exercise of that right does not, of itself, justify the Security Intelligence Service in instituting surveillance of any person or entity or any class of person or entity within New Zealand.
- S.4AA requires the Service to limit its activities to those relevant to the discharge of its functions, requires that it be left free from any influence or consideration not relevant to its functions and removes any party political focus of the Service's work.
- s.4A requires specific authority for collection of information by interception or

seizure.

- s.4F requires minimization of the impact of interception warrants on third parties.
- s4G requires the destruction of irrelevant records obtained by interception ie what may be retained when obtained in that way must relate directly or indirectly to the detection of activities prejudicial to security or be foreign intelligence information essential to security.
- s.4H provides particular authority for the Director to retain and to release information to the Police or any other person for the purpose of preventing or detecting serious crime in New Zealand or overseas. That power is general and not subject to a qualification related to security.

11. (ii) **as to personal privacy:** Section 57 of the Privacy Act 1993 is a recognition that intelligence organizations may have a need to obtain information relating to individuals, the collection or holding of which would be constrained by the general privacy principles in the Act. There are twelve principles set out in the Act. Only Principles 6, 7 and 12 apply to intelligence organizations. Principle 12 controls the use of unique identifiers. Principles 6 and 7 allow an individual to obtain confirmation whether personal information is held about him or her, to have access to it and to seek correction if necessary.

Requests for confirmation about holdings may however be refused on grounds, amongst others, of prejudice to security or defence or international relations, prejudice to the entrusting of information to the Government on the basis of confidence by overseas bodies, and prejudice to the prevention, investigation and detection of offences.

The Privacy Act request procedure is used. Requests to the Service increased from 10 in 2007 to 303 in 2009. Each request can require a declassification process and perhaps assessment related to the privacy of persons other than the enquirer as well as copying and supplying material and, for good reason, keeping a record of what information has been supplied. That record is now presenting its own storage problem.

12. (iii) **as to records generally:** The Public Records Act provides an over-riding general control of the disposition of public records, which would include those held by the NZSIS.

Internal controls:

13. The Service has internal rules and practices about access to information held by it which are designed to ensure that the information is held securely. There is a general requirement on staff and assistants not to disclose or use what they become aware of in the course of their duties. That is backed up by the criminal sanction in s.12A of the NZSIS Act 1969. There are internal restrictions on access to information, including designation of managers as access right holders, designation

in some cases of groups of officers who alone may have access to information depending on its level of sensitivity, and the need for permission from access right holders to be sought by non-designated officers who consider that for official work they have a need to know controlled information. This process is a buffer between the needs to control access to information and to share knowledge within the Service.

Changes in recording methods:

14. The Service and its predecessor originally operated with paper files. Since 2005 it has operated with electronic records in systems designed to allow access to information by those who need it and to protect the information from misuse and access by those who have no need for it. A current problem being addressed by the Service is to develop access so that as much relevant information as possible is available to assessors and decision makers, rather than access to information being limited to parts of the Service with particular responsibilities. An essential part of such change will be to ensure that information continues to be protected despite wider access. *This is a work in progress and advice has been sought from people with relevant wide experience.*

Destruction of records, in the full sense of that term, is less easy to achieve when they are in electronic form than it was when they were paper-based. The Service seeks to achieve the same effect by controlling access on a need to know basis and eventually, after proper assessment, removing the possibility of access to particular information altogether. That approach I believe meets the realities presented by the technology both in terms of cost and in terms of concern about building up personal dossiers for what might be seen as inadequate security reasons.

The nature of intelligence:

15. A U.K report has given this description:

"Secret" intelligence is information that is lawfully gathered by the Agencies, but without the consent of the target. It can come from an individual, an organization, or a country. Intelligence, as defined by the security Agencies, can include anything from a recruited agent or intercepted telephone calls to covert eavesdropping in a person's home. Intelligence has to be assessed to decide how reliable it is, including the reliability of the source. It also has to be analysed to decipher which facts are important and which are not. There are many limitations to intelligence – it may be very fragmented and only give a partial picture. It rarely gives the full story and so there will inevitably be gaps in what [...] Agencies know at any given time".

UK Intelligence & Agencies Security Committee review of the intelligence on the London Terrorist Attacks on 7 July 2005 Cm.7617 May 2009.

16. It is generally accepted, and indeed seems self-evident, that information collected

will have varying degrees of value over time, including a change in value when associated with later acquired information. It is also generally accepted that intelligence issues may require development of a picture over time.

Control of collection of information:

17. One of the concerns giving rise to this inquiry has been continued collection in the past about individuals once they became, for whatever reason, recorded in the system as persons of interest. Some are concerned that they have become persons of interest at all; others are concerned that they may suffer some detriment if information about them is not strictly controlled. An approach of creating categories within which information could be collected has been considered by a group of Service officers. As a system it is seen as not achieving more than the system which has been developed.
18. It is I think fair to say that any detailed prescription of what the Service may collect is likely to be difficult in definition and to present difficulty in decisions as to whether particular information is within the definition.
19. The Service's approach has become to emphasise in its procedures task-orientated gathering of information. Investigations are conducted under an investigation framework introduced in 2009. The pattern of that framework provides that the investigation must fit the Service's strategic domestic security intelligence objectives and priorities which are reviewed annually. It requires:
 - statement of an investigation objective and the benefit expected to be produced by it.
 - an indication of what has led to the investigation being proposed.
 - a statement of what investigative action is proposed and what information will be sought.
 - a statement of any anticipated problems.
 - a timeline and date for review of the investigation.
 - at the designated time a review is undertaken of what has been done and an assessment is made of what has been achieved. A decision is made as to whether the investigation should be taken further.
20. If the answer to that question is negative, the investigation is closed. At that stage records will be closed. Such closure may come about because the objective has been achieved or because the particular investigation is judged to be lower in priority than others for which resources are required. At the stage when an investigation is closed, particularly if that is related to competition for resources, the possibility of re-opening exists if priorities change or new related information relevant to security

emerges. A closed record still carries any access control tags it has had.

21. In addition to what is discussed above, regular reviews are made by managers of priorities amongst a group of current matters, which helps to clarify the focus on what is and what is not being investigated.
22. In addition to the investigation framework, the Service has an information management policy and statement of procedures, last revised in 2008. Further revision of it is also a work in progress. The 2008 revision included criteria in respect of personal records, at least one of which must be met before a personal record can be created. The two most immediately in point are:
 - The individual's activities must fall within the collection requirements of the Service, and a valid reason tied to those requirements must exist for obtaining detailed information about that person or about the part he or she plays in a target organization;
 - The individual is engaged in activities relevant to security which justify further investigation for assessment purposes.
23. *These two lines of control (paras 19 and 22) have the effect in my view of sharpening the focus of collecting information by reference to the statutory security criteria in respect of present and possible events rather than to activity of particular persons which may not be clearly security related. So long as a consistently disciplined approach is applied at the start of collection about any person and a similar approach is taken to any addition to a record, what would now be seen as unnecessary collection of personal information should fall away.*

Control of retention of information:

24. What is useful information for intelligence purposes reflects the nature of intelligence (described in para 15 above). When it relates to a matter within the statutory security criterion it may have value:
 - when the investigation is alive, which may be for some time.
 - as support for any intelligence report made as a result of investigation.
 - as information relevant to new developments or patterns of behavior, particularly when light is shed by new information on old or by old on new.
 - providing a research tool for the Service.
 - providing an historical context for continuing categories of risk or recording operational practice. The historical context is regarded as very important.
 - providing a working basis for any revived investigation ie not having to go over old ground again.

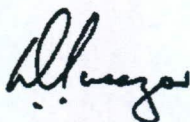
25. The system emphasises that criteria must be met for opening a record. No particular criteria have been developed (or possibly can be developed) for reviewing the continued holding of personal information, other than age and continuing relevance to one or more of the aspects of security intelligence work referred to above. Thus the information management policy contemplates the closing of personal records to which there has been no need to have access for five years and when there is no suggestion of current security interest. A manager's authority would be required to add anything to such a record. Once it is determined that there is no security interest (or better, no security related reason for interest) links in the electronic system to the personal information will be closed.
26. The five year period is a matter of choice, and replaces the three yearly review thought appropriate in 1995, but I have been advised and accept that making too short the period for holding information which there has been a security-related reason to collect, and approaching the matter on an across the board basis, create the danger of losing information which still has value for security purposes, and thereby damaging the performance of the intelligence functions. One of the resource problems in the discarding of material is that a proper assessment of what can go may require the judgment and expertise of people experienced in intelligence work.
27. In respect of existing hard copy files, a disposal authority under the Public Records Act has been granted by Archives N.Z covering old vetting records. Disposal authorities in respect of old subject files, some of which relate to organizations of interest in the past, and files relating to people have been under discussion. Getting authority to destroy is likely to be a drawn out process. Privacy considerations I should think would provide an argument in favour of the destruction of personal information collected for a particular purpose and no longer required. In the public record area however, arguments are made by historians and others for retention of records because of perceived historical value. It is not irrelevant that the Service's experience has been that many people who have made personal information requests have indicated a preference that material be placed in archives rather than destroyed.
28. Disposal one way or another of what has no appreciable current security value is unlikely to be achieved in a short term. By 2006 the Service and its predecessor had accumulated, over considerable time, records relating to some 6,700 individuals (by no means all of whom are NZ citizens).

Information supplied by the Service:

29. The Service's business is not the supply of raw data but is the supply of assessed intelligence relating to its tasked areas. Its work includes asserting control of the use of information which it supplies, whether to organizations in New Zealand or to liaison partners overseas. That is done by means of security classification and caveats imposed by the Service, which control the use to which supplied information may be put. Its records include information about who has been told what. Caveats are an important aspect of the intelligence function. The sanction for not observing them may be the end of the supply of information. This has been extensively discussed by Courts in the United Kingdom, which have accepted that the possible consequences are a reality.

30. Summary:

1. The Service is in the process of discussing disposal of old hard copy records. This is not going to be a short term exercise.
2. Current collection of information is related to tasks within a framework of investigation in respect of potential or actual threat covered by the statutory definition of "security" and to persons in respect of whom there is a valid security reason for enquiry. That is a control mechanism having effect at a significant point in the Service's activity.
3. As resources allow, more controls will be developed in respect of access to information held by the Service so that it is securely held but available to those who need to have access to it.
4. The Service should in time achieve disposal and in many cases physical destruction of old records relating to individuals, in so far as that is allowed under the Public Records Act procedures and authorities.
5. With electronic recording, continuously closing off access to records which no longer reasonably serve a security related purpose is possible. Even if physical destruction is not feasible, electronic techniques which have the same practical effect are being pursued. Some form of "shelf life" approach to such a process (subject to the qualifications discussed), seems likely to provide the best way to keep the retention of information down to what is necessary for purpose.
6. In view of the expressed concerns about what personal information might be held by the Service, it would be useful in terms of public confidence if the Service's annual report affirmed with such detail as is appropriate that destruction of or closing access to dated records is a continuing process.



D P Neazor
Inspector-General