Office of the Inspector-General of Intelligence and Security

Review of NZSIS holding and use of, and access to, information collected for security vetting purposes (Part one)

Public Report: Summary and Conclusions

Cheryl Gwyn
Inspector-General of Intelligence and Security

7 April 2016

Vetting function of the Service

1. The New Zealand Security Intelligence Service ("Service" or "NZSIS") has an express function under s 4(1)(bb) of the New Zealand Security Intelligence Service Act 1969, to conduct inquiries into whether particular individuals should be granted a New Zealand government security clearance. The assessment ("vetting") of candidates for security clearances is necessary to limit the risk of protectively marked information being accessed by unauthorised organisations and persons.

2. The investigations undertaken by the Service in discharging that function are necessarily highly intrusive. The information collected in the course of vetting includes personal information relating to, among other matters, sexuality, social habits, physical and mental health, financial wellbeing, and religious and political affiliations. The consolidated records collected during the vetting process likely comprise the most sensitive repository of such personal information held by the New Zealand government. Any inappropriate use or unwarranted disclosure of that information could have serious implications for the subject of that information and others.

3. Under s 11(1)(d)(ii) of the Inspector-General of Intelligence and Security Act 1996 (IGIS Act), I am required to review the compliance systems of the NZSIS and the Government Communications Security Bureau ("GCSB"). As one part of that ongoing process of review, I have undertaken an examination of the Service's systems for storing, using and controlling access to information that it compiles for the purpose of assessment ("vetting") of candidates for New Zealand government security clearances.

4. I have decided to report on that review in two parts. Part one of the report sets out:

    4.1. The background and purpose of the review, the process followed, a summary of my findings and consequent recommendations;

    4.2. An introduction to security clearance vetting and the information compiled;

    4.3. The measures taken for secure storage of and control of access to that information;

    4.4. The purposes for which information compiled for vetting may be used and the circumstances in which information may be disclosed; and

    4.5. Conclusions concerning current Service practices.

5. I decided to report on this review in two stages because I had identified a number of significant concerns around physical storage, use and access controls, and wished to raise those promptly so that those problems could be identified and addressed as quickly as possible. I expect to complete the part two report, which will address remaining aspects of this review relating to electronic record storage, in coming months.

6. I provided the part one report in draft to the Director of the Service, in accordance with the requirement to give an opportunity for response on adverse findings under s 19(7) of the IGIS Act. In addition to providing comments, which I have considered and as appropriate incorporated into the finalised first report, the Director has confirmed her acceptance of my recommendations. Some of those can be implemented immediately while others will take some time. The Service has, since the first report was concluded, removed the dual managerial role and the separation between vetting teams described here.

7. I expect to continue to work with the Director and the Service on the implementation of these recommendations and will continue to report on that outcome to the Minister and in my next annual report.

Background and purpose

8. I undertook this examination for four reasons:

   8.1. **The scale of security clearance vetting:** The assessment of security clearance candidates is a significant aspect of the Service's functions, both because it is a key safeguard for national security information and because the Service's contact with security clearance candidates and with others, interviewed as part of the clearance vetting process, is the part of its work that is visible to the widest number of people. There are, at any given time, some thousands of people with New Zealand government security clearances, as well as many others who have held clearances in the past.

   8.2. **The breadth and sensitivity of information potentially relevant to security clearance decisions:** The security clearance vetting process compiles a very wide and detailed range of information about each candidate's working and personal life. In accordance with the New Zealand Government Protective Security Requirements, the relevant information encompasses such potentially sensitive matters as potential alcohol or drug dependency, mental health conditions and personal and financial matters. In some cases, security clearance vetting information will also include classified intelligence information. In order to meet the Service's own obligations of information security, meet the assurances that the Service gives to those providing information and to secure and maintain the confidence of clearance candidates, clearance holders and referees, the sensitivity of such information must be reflected by appropriate safeguards.

   8.3. **The exceptional scope of information-gathering for security clearance procedures:** While candidates are not under any legal compulsion to provide such information, failure to provide all relevant information may well result in refusal of a clearance and consequent loss of or failure to obtain employment. Security clearance decisions are also partially exempted from anti-discrimination law, and for both reasons may encompass information that could not generally be obtained by an employer.[1] The records compiled in the process of security clearance vetting, particularly higher levels of clearance, are the broadest compilation of sensitive personal information held by the New Zealand government. There is also an obvious risk that an adversary may seek to

[1] See Human Rights Act 1993, s 25, exempting restrictions on the employment of any person on work involving the national security of New Zealand from several grounds of proscribed discrimination.

access such sensitive personal information as a means of identifying and/or compromising persons who hold security clearances.

8.4. **The need for clarity around any use of security clearance information for any other purpose:** Some, though not all, of the guidance given to security clearance candidates and to referees suggests that information compiled for security clearance purposes will be used only for that purpose. In the course of several reviews and inquiries into Service activities, however, I have become aware of some instances in which security clearance vetting information appears to have been used for other purposes, as confirmed by the Service.

9. Since I commenced this review, the need for confidence and clarity in the security of such information has been highlighted by the disclosure that the United States' systems for its security clearances was the subject of a data breach of personal details of more than 22 million people compiled over at least 15 years of background checks.[2] There is not, so far as I am aware, any allegation of a similar breach, or attempted breach, in respect of the Service's records and, as a review of Service systems, my review has not canvassed any possible breach or other of improper use or disclosure. The second part of the review report will address some further aspects of electronic record-keeping, including some limited testing of access that my staff were able to undertake.

10. I have not addressed security clearance decision-making in this review, other than to the extent that it bears on information handling.

Process followed

11. On 27 January 2015 I wrote to the Director of the Service seeking information to inform my review of the Service's holding and use of, and access to, information collected for security vetting purposes.

12. In the course of the review, members of my staff met with, and obtained various information from, a number of Service staff from the two vetting divisions – those with responsibility for intelligence community (IC) vetting and those responsible for all other vetting, termed "Customer vetting"[3] – and Service human resources and information technology staff. We also searched for any Service policy and/or procedure documents that deal specifically with storage, use and disclosure of security clearance information, but found there to be only very limited material of this kind.

13. As the review progressed, we identified aspects of the Service's practices around security vetting information that, in my view, required change. It also became clear that the investigation of some aspects of electronic record-keeping, including undertaking limited

---

2 United States Government, Office of Personnel Management "Information about OPM Cybersecurity Incidents" (https://www.opm.gov/cybersecurity, visited 7 August 2015); see also, for example, D E Sanger "U.S. Decides to Retaliate Against China's Hacking" *New York Times*, 1 August 2015 and *USA Today* "OPM's cybersecurity chief resigns in wake of massive data breach", 22 February 2016.

3 Structural changes commenced by the NZSIS since conclusion of the part one report include change to the separation between these two vetting groups.

testing of access to records, would require additional time. I therefore decided to report on this review in two parts.

14. I am grateful to those Service staff who have given much of their time over recent months to meet and correspond with my investigators.

Information subject to national security restrictions

15. In accordance with ss 13 and 25(8) of the IGIS Act, I have considered the security classification of the first report of this review, which has required me to determine whether any of the content of the report would, if disclosed publicly, be likely to harm national security. As part of that process, I have consulted the Director of the NZSIS concerning the classification of the first report and reference to NZSIS classified materials, as required by s 25(8).

16. I have determined that there is some limited detail of NZSIS systems and practices that would, if disclosed, be likely to harm national security:

    16.1. The specific detail of NZSIS physical and electronic file storage systems and practices, as public disclosure of that detail may put the security of those systems at risk. That information includes excerpts from NZSIS classified material subject to s 25(8)(b); and

    16.2. The specific detail of some of the shortcomings that I have identified, where publication of that detail may disclose or highlight a vulnerability that could be exploited or that could, through a loss of confidence, impair Service capabilities.[4]

17. As a result, and to the extent strictly necessary to avoid that likelihood of harm, I have established that that information should not be disclosed publicly. As the Service completes its work to address the recommendations made in the first report, at least some of the vulnerabilities will be removed and it will be possible to disclose those details at that time.

18. The full classified first report has been provided to the Minister in charge of the NZSIS and the Director of the NZSIS. I have also provided the full classified first report to security-cleared representatives of a number of government agencies that have a particular interest in security clearance practices.

Findings and recommendations

19. I have examined the Service's practices and safeguards that govern the secure storage, accessibility and use of information concerning security clearance candidates.

20. I have found that the Service and Service staff working in the vetting area are conscious of the sensitivity of vetting information and those staff have emphasised to me the importance of personal integrity and discretion. Responsible staff sign a written undertaking about

[4] The practical reality of such risk of disclosure may have been demonstrated in the United States data breach at n 2 above. News accounts of the investigation of that breach have suggested that some detail contained in a published audit of IT security may have assisted one part of the breach: see, for example, National Public Radio "U.S. Officials Say Nearly 14 Million Affected in OPM Breach" 15 June 2015.

permissible use of information. Staff responsible for decisions around use of information, such as the sharing of vetting information with other parts of the Service and the disclosure of particular information to sponsoring employers, have also emphasised the care with which those decisions are made.

21. What is also necessary, however, to supplement and allow verification of the steps taken by individual staff, are the following: [5]

    21.1. Secure receipt and storage of that information, consistent with its highly sensitive nature and the attendant risk of compromise;

    21.2. Physical and electronic access controls consistent with the "need to know" principle;

    21.3. Regular auditing of access to each record and file, which in return requires logging of access and of the reasons for that access; and

    21.4. Robust standards and decision-making procedures for any other use of such information, including disclosure, and safeguards to ensure proper use of that information. Candidates, referees and others who provide information to the Service for security vetting purposes should be informed of, and consent to, any potential use.

22. These four points are addressed in turn.

Secure receipt and storage

23. For clearance decisions for its own staff, those of the GCSB and some others (termed "IC vetting"), the Service uses predominantly physical files, together with some limited electronic information held in the Service's document management system (DMS). For all other ("Customer vetting") vetting clearance recommendations, the Service uses electronic records. Physical files are held under secure conditions.

24. Electronic information received and/or generated is held on four systems: the Online Vetting Request (OVR) system; a case management system for working with vetting information; the DMS; and, for limited information about all candidates and referees, a records system generally accessible to NZSIS staff.

25. As noted above, some aspects of electronic record-keeping will be addressed separately in part two of the report of this review.

Access controls

26. All Service staff sign agreements about the use of IT systems, which specifically refer to permissible use of those systems and, for example, prohibit use of Service data for personal

[5] See both New Zealand Government, *Protective Security Requirements* "Personnel security management core policy" (personnel security clearances supplement, not replace, "correct application of the need-to-know principle, access controls [and] information security measures") and Office of the Privacy Commissioner *Data Safety Toolkit* (2014ed) 13 (need to "[k]eep files separate … put in place access controls; [m]ake sure electronic files can be audited and carry out those audits routinely; … limit access to personal information on a need-to-know basis").

or other improper purposes. Further, physical files are held in defined areas and particularly sensitive and dormant/historical files are each held separately.[6]

27. However, there are not comprehensive access controls. For the hardcopy files used for IC vetting and with the exception of those files held separately, all staff responsible for IC vetting have physical access to all "active" vetting files.

28. The electronic records that are held on the DMS are held in several access control groups (ACGs), which are each accessible by different groups of Service vetting and related staff. There is some compartmentalisation: records for IC vetting are accessible only to IC vetting and certain other staff and particularly sensitive records, such as those for senior managers and for the vetting staff themselves, are accessible only to a smaller group of responsible staff. However:

    28.1. All Service vetting and related[7] staff have access to vetting-related DMS files for all customer vetting.

    28.2. All IC vetting and related staff have access to vetting-related DMS files for all IC vetting, other than the particularly sensitive records.

    28.3. Within these arrangements, vetting-related DMS files remain accessible whether or not there is any current reason for access. While some files are reviewed and/or updated regularly, many need to be accessed only approximately every five years, when clearances are reviewed, if still needed. DMS files for people who have held, but no longer hold, clearances remain accessible to vetting and related staff, whether or not there is any specific need for that general access.

29. Some counter-intelligence staff also have access to some security clearance vetting documents.

30. For the other electronic systems:

    30.1. Files held on the case management system are accessible to all vetting and related staff.

    30.2. As discussed separately below in relation to use of vetting-related information, some biographical information about candidates and referees is held in the records system accessible to all Service officers.

    30.3. Scanned pre-2009 vetting files are also held in that system but with access restricted to all vetting and related staff.

31. For the most part, only a handful of Service vetting and related staff require access to each particular file and most files do not need to be accessible at any given time. However, the practical result of the current limited access controls is that the largest compilation of vetting records – those relating to all candidates assessed by Customer vetting, who

[6] Some pre-2005 physical files were destroyed after ten years of inactivity.

[7] "Related staff" are other staff with vetting-related responsibilities, such as some legal and IT staff.

comprise thousands of people – are accessible to approximately 60 Service staff. The second largest compilation of vetting records – all those relating to most candidates assessed by IC vetting, amounting to some thousands of people – are all accessible to approximately fifteen of those staff.

32. So as to comply with the information security principles that I have set out above, I recommend that:

R1. The Service should adopt more focussed access controls on vetting information, so that vetting and related staff each have access only to particular physical and electronic records to the extent reasonably necessary at the time. Given the inherent difficulty in limiting access to physical files and the comparative ease of regulating electronic access, it may be most straightforward to move IC vetting more completely from physical to electronic files.

R2. In order to safeguard individuals' privacy and in line with the assurances and consents given, the Service should limit the information that is generally accessible by Service officers about candidates and referees obtained from vetting to those individuals' names and dates of birth, to allow for identification, together with a flag that further information is held on a vetting file. Address or other information from that vetting file may then be sought under the Service's use/disclosure procedure.

Audit of access

33. So far as individual physical files are concerned:

33.1. Active (working) files are held in the vetting staff area of the building. There is no recording of access to individual files or reasons for access.

33.2. Inactive files for current clearance holders and recent clearance candidates are held in separate secure storage and access to the storage area is logged. Where a file is removed from that separate storage area, that is recorded on a transit card. However, there is no recording of review of particular files within the secure storage area or of reasons for access to particular files.

33.3. Archived files – those relating to former clearance holders – are held in a second separate area. Access to that area is restricted. There is no recording of access to individual files in that area or of reasons for access.

34. For electronic records, access recording and auditing is inadequate.

35. While I acknowledge the emphasis placed by Service vetting and related staff on their personal integrity and discretion, there is not an adequate objective check or assurance that records are never accessed for unauthorised or improper purposes. So as to comply with the principles set out above, I recommend that:

R3. The Service move to ensure recording and regular audit of access to, and reasons for access to, all categories of vetting information files. Given the comparative ease of logging and auditing access to electronic files, it may, subject to any issues that may

arise in the part two report, be most straightforward to move to use only electronic files.

Decisions concerning use of vetting information for other purposes and disclosure of information

36. The use and disclosure of vetting information beyond vetting recommendations raises difficult questions:

    36.1. As I have noted, the information provided by candidates, referees and others is highly sensitive and candidates are practically obliged to provide information, some of which they would not otherwise ever have reason to disclose. The particular character of vetting information, and the Service's requirement for absolute candour, is acknowledged by the Service in the various assurances given to referees and candidates and the terms of consents that are sought.

    36.2. There are circumstances in which use of vetting information for purposes beyond vetting assessment, including possible disclosure, may be justified. In particular, it appears reasonable that, where the holder of a security clearance becomes the subject of a counter-intelligence investigation, some information from that person's vetting record may properly be used for that investigation. However, other use – for example, use of vetting information for general intelligence purposes - is likely to be unjustifiable.

37. In order to balance those two considerations:

    37.1. Vetting information may be used for other purposes only where the other purpose is shown to be sufficiently compelling to warrant the use of such information, bearing in mind its sensitivity and the circumstances under which it is obtained.

    37.2. Where information is provided within the Service for a specific purpose or disclosed outside the Service, there are appropriate safeguards to ensure that it is not used for other purposes.

    37.3. The assurances given to, and consent sought from, candidates, referees and/or others who provide information should unequivocally acknowledge any potential use and/or disclosure.

38. The Service has an existing procedure for the use of information from vetting files for other purposes, under which information can be accessed for another purpose only after application to the responsible Deputy Director, who must be satisfied of the intended purpose, though it appears to be rarely if ever used. However, I identified a range of other practices by which vetting file information is accessed for various purposes, some with access controls and some form of assessment of justification, and others without.

39. The Service also advises candidates and referees about the use and confidentiality of information provided, in the form of various assurances, consents and other statements. However:

39.1. There is some inconsistency in the terms of different forms of advice, both as between different stages of the vetting process and between the terms used by IC and Customer vetting.

39.2. While there is an *aide memoire* for Service vetting interviews that includes an explanation of the potential use of information, Vetting Officers may currently give that explanation in their own words, leading to an avoidable risk of inconsistency or misunderstanding.

39.3. Some of the current use of vetting information set out above is not consistent with the assurances, consents and other statements as made.

40. I therefore recommend that:

R4. The Service should ensure clear standards and procedures for any use of vetting information outside security clearance assessment. Any decision to use information for other purposes – whether in a particular case or in relation to a particular category of information – should be made consistent with the new standards and procedures and at an appropriately senior level, so as to ensure that use can be shown to be justified and that attendant safeguards are in place.

R5. All of the existing arrangements for other use of or access to vetting information should be reassessed against those new standards and procedures and continued only if, and to the extent that, they are found to be justified and subject to appropriate safeguards.

R6. The Service should develop safeguards against the risk of unfair use of information obtained from security clearance procedures by an employer, including by the Service or Service managers where the Service is the employer. For security clearance assessments involving staff with responsibility for security clearance vetting, the Service should – so far as possible[8] – ensure that a line manager is not responsible for both an employment decision and approval of a vetting recommendation and that the decisions are not conflated.

R7. If the use of pre-emptive risk advisories is retained, whether in the form of Security Risk Advisories as used in the past or otherwise, express standards should be put in place to govern their use and content. This will provide for consistency in the triggering thresholds and a considered approach to assessing the extent of disclosure necessary to satisfy the risk mitigation purpose of the advisory, weighed against the potential consequences of the disclosure to the candidate and potential safeguards.

R8. Advice to candidates, referees and others about all potential use and/or disclosure of information provided for security vetting purposes should be consistent and unequivocal. Advice concerning use and disclosure given at interviews should follow a common text.

[8] For example, the Director will have ultimate responsibility for appointment and clearance decisions for senior positions within the Service. The Service has advised that the Director will obtain legal advice to ensure separation between the two decisions in such cases.

Other

R9. The inconsistency in relevant practices between the two Service divisions responsible for security clearance vetting, including the differences in the management of candidates' information, should be addressed. I acknowledge that the Service has implemented structural changes intended to have that effect.

Continuing review

41. I anticipate working through the issues that we have identified with the Service, including where the Service has – as I have noted – already initiated its own reviews and reforms. There are significant points of strength in the Service's practices and concerning the management of vetting information and I am confident that the recommendations I have made will assist in building upon those strengths and remedying those areas where systems are inadequate.