Office of the Inspector-General of Intelligence and Security

Summary guide: Putting procedural fairness into practice in NZSIS security vetting

---

Cheryl Gwyn
Inspector-General of Intelligence and Security
November 2016

Contents

Introduction

1. One of the primary functions of the New Zealand Security Intelligence Service (NZSIS or the Service) is to carry out security clearance assessments – also known as "vetting" – for people who need access to security classified New Zealand government information as part of their work. The basic objective of the security vetting process is to determine whether the person concerned – called a "candidate" – can be trusted not to disclose that information.

2. The process of security vetting canvasses a wide range of personal attributes in order to determine if the candidate has the necessary degree of personal integrity and is not unduly vulnerable to coercion or other adverse influence.[1]

3. The need for fair and robust decision-making in security vetting is plain. From the perspective of the New Zealand government, the unsound conferral of a security clearance may lead to disclosure of information that threatens national security, endangers lives or harms New Zealand's international relations. For each individual candidate, an unfair NZSIS assessment can lead to unjustified loss or denial of employment, harm to reputation and risk work and personal relationships. And for the candidate's employer or sponsoring agency, unsound decisions can cause security risks or, conversely, the loss of a key staff member.

4. Fairness is required by law.[2] It is also a critical part of a robust security vetting process, as recognised in the New Zealand government's *Protective Security Requirements (PSR)*.[3] The practical necessity of fair process is also clear. As put in a leading case, fair process is a key means to recognise and address:[4]

> "… examples of open and shut cases which, somehow, were not; of unanswerable charges which, in the event, were completely answered; of inexplicable conduct which was fully explained; of fixed and unalterable determinations that, by discussion, suffered a change."

5. That need is particularly true for security vetting, given the sensitivity and subtlety of much of the information concerned and the stringent standards to be met.

6. This *Guide* draws together extensive work undertaken by the Office of the Inspector-General in the investigation of complaints by people against whom the NZSIS had made adverse or critical assessments. As noted in the Inspector-General's 2014-2015 *Annual Report*, those investigations indicated that while the NZSIS staff had followed what they had understood to be their procedural obligations, NZSIS practice and the content of the *PSR* fell short of what was required by law. The *Guide* is not a substitute for legal advice for the NZSIS or for candidates, but sets out the NZSIS's obligations and how those obligations can be effectively met.

---

1 See, further, New Zealand Government *Protective Security Requirements* (accessible online at https://www.protectivesecurity.govt.nz) S4.

2 *Greene v McElroy* (1959) 360 US 474, 508; *Thomson v Canada* [1992] 1 SCR 385, 402; *Home Office v Tariq* [2012] 1 AC 452, [27] and see further *Annual Report* (accessible online at http://www.igis.govt.nz) at pp 15-17.

3 Above n 1, *Personnel Security Management Protocol: Procedural Fairness Requirements*. The *PSR* sets out a number of aspects of procedural fairness and describes it as "an essential part of security vetting." However, the *PSR* does not currently address all applicable legal obligations and is equivocal in some respects. The NZSIS has committed to reforming its practices in line with those obligations and as reflected here, both in current changes to its working practices and by revising and expanding the *PSR*.

4 *John v Rees* [1970] Ch 345, 402 approved in, for example, *R v Guy* [2015] 1 NZLR 315 (SC), [45].

Fairness in NZSIS security vetting: a practical summary

7. Fairness in security vetting has three components.

Taking all reasonable steps to obtain available relevant and reliable information

8. The NZSIS, with appropriate assistance from the employing agency in line with the *PSR*, must take all reasonable steps to obtain accessible information that is relevant to its assessment and, particularly, to any identified issue of potential concern. Extensive steps will be appropriate, particularly where any concern arises:

    8.1. If it is necessary to investigate workplace conduct, the NZSIS must obtain relevant employer personnel files or other records;

    8.2. Similarly, if material financial or health issues arise, NZSIS must obtain relevant records;

    8.3. Where opinion is obtained, NZSIS must investigate the underlying facts; and

    8.4. Where an issue involves expert judgement – for example, evaluations of financial propriety, mental health, or substance addiction – expert opinion is necessary.

9. The NZSIS must make an objective assessment of the reliability and currency of any information before taking it into account, especially in respect of information obtained from referees. Where particular information cannot be disclosed, NZSIS may only rely upon that information in exceptional cases and, in such cases, must take particular care.

Disclosure to the candidate and an adequate opportunity to respond

10. Where an adverse assessment is possible, but before forming any concluded view:

    10.1. The NZSIS must disclose that possible assessment and all relevant information, both positive and negative, to the candidate.

    10.2. Certain information can be withheld, but only where certain narrow criteria are satisfied. Most commonly, in this context, that will be where an evaluative statement has been given in confidence or where disclosure would threaten national security or personal safety. As much information as possible must be provided in such cases.

    10.3. The candidate must be given an adequate opportunity to respond, including by oral and/or written comment on the adverse assessment and relevant information and to present further information. Where expert opinion is relied on, the candidate is entitled to answer that by obtaining his or her own expert response. The NZSIS must assess any response with an open mind, including through further investigation where new questions arise.

Objective and reasoned assessment of information obtained

11. The NZSIS must assess all of the information obtained, both positive and negative. The eventual assessment must set out the reasons for the conclusion reached in terms of the applicable criteria. The factual basis for any assessment or opinion must be set out and, where there is contradictory information or where information has been disregarded or seen as outweighed, that must also be noted and explained.

Obtaining all reasonably available, reliable and relevant information

12. NZSIS is obliged to obtain and evaluate all available, reliable and relevant information, taking all steps to obtain such information that are reasonable in the circumstances, including but not limited to ensuring that candidates' employers provide the information required from them under the *PSR*.[5] Because of the gravity of security clearance assessments, extensive steps will be appropriate where necessary to resolve an issue or concern.

13. The steps that NZSIS must take will vary according to the nature of any issues that arise, but by way of likely common examples:

    13.1. NZSIS must consider whether there are or may be available records of any matter of concern. For example, if a concern arises around workplace conduct generally or a particular incident in the workplace, any records held by the relevant employer should be obtained;

    13.2. Where relevant records are not kept but information can be made available, for example where managers can provide an account of an incident, that should be obtained in a form that can be shared with the candidate; and

    13.3. Where any issue of expert judgement is material, for example around mental health or complex financial matters, NZSIS must seek an appropriate expert opinion.[6]

14. Where information is identified as relevant but records have been lost or cannot be collected, the NZSIS should consider whether there are steps to mitigate that loss, for example by asking the agency or person responsible to provide a formal statement or working with the candidate to piece together available records.[7]

15. Where the NZSIS is provided with impressions, opinions or interpretations, those should not be used as primary reference material in themselves but as a starting point for the collection of factual information and NZSIS's own analysis.

Seeking information by the most authoritative means

16. As NZSIS strives to obtain all available and relevant information, this process should be conducted formally and must not involve seeking information by informal means, for example by an undocumented request or an approach to a contact at the employing agency.

17. In particular, where information is required concerning any issue of serious consequence, the NZSIS should take the most authoritative means of obtaining that information. For example, where there is an allegation of workplace misconduct or of a security breach or incident, the most authoritative means is likely to be a request to the employing agency for its records or, if necessary, for a statement made on behalf of the agency.

---

5 See, for example, *CREEDNZ v Governor-General* [1981] 1 NZLR 172 (CA), 200: "… the decision-maker should not be misinformed as to established and material facts, including in that expression incontrovertible expert opinion; … [the decision-maker] must take reasonable steps to acquaint [him- or herself] with the relevant information."

6 See, for discussion of good practice, the United States *Adjudicative Desk Reference* (United States Department of Defense, 4ed 2014), 256, 310, 320, 377, 378 & 379.

7 See, for good practice, Australian Government *Personnel Security Guidelines: Vetting Practices* [6.4] pp 54.

Obtaining appropriately qualified assistance on matters of expert judgement

18. Where an issue involves an assessment of a candidate's mental health or other questions that involve clinical or other expert evaluations, NZSIS must obtain assistance on that assessment from an appropriately qualified expert as to both:

    18.1. Whether the candidate has, for example, a particular mental health condition and the gravity of that condition at the time of the NZSIS assessment; and

    18.2. What implications, if any, that condition has in terms of security risk vulnerabilities.

19. The critical role for NZSIS is to ensure – both at the time of seeking expert advice or opinion and once it is received and applied – that the advice or opinion is robustly informed, reasoned and relevant:

    19.1. The expert has access to all information that he or she considers relevant, including any contradictory information;

    19.2. The expert's advice or opinion sets out the information relied upon and the criteria applied in reaching any conclusion(s); and

    19.3. The expert's advice or opinion explains how those conclusions correspond to security risk criteria.

20. Once NZSIS has obtained the necessary advice or opinion, including pursuing any outstanding issues or questions that may arise, it should be straightforward to apply the conclusions reached as part of the vetting assessment. Disclosure of expert advice or opinion to candidates and disagreements between experts are dealt with on page 11 below.

Assessing reliability and currency of information provided

21. NZSIS must assess the reliability and currency of any information before relying upon it and, where any question arises, must investigate that question. That entails:

    21.1. An objective assessment of whether there is any indication that the particular information may be unreliable or outdated;

    21.2. Where there is an indication of possible unreliability of some information, details should be sought about the source of the information and by corroboration; and

    21.3. Where investigation indicates that information is not reliable, or uncertainty cannot be resolved, or the information cannot be independently and reliably corroborated, that information must be put to one side. One narrow exception is discussed below.[8]

22. To ensure the reliability of information is assessed effectively, it is important to take a broad view of potential reasons for unreliability. Any objective indication should be investigated, including any internal or external contradiction or inconsistency in the particular information itself; where it appears that information may be outdated or incomplete; and any material limitation or motive on the part of the source of the information.

23. In the particular case of statements made by referees, any significant motive is relevant, whether positive or negative, and should be investigated and taken into account. That can encompass, for instance, not only whether a referee might stand to gain from the outcome of the security vetting process but also personal or professional affection or dislike; family, career or other connections; or past perceived advantages or slights. It is also necessary to recognise that such motives are not necessarily consciously malicious: for instance, a referee who is a professional colleague may sincerely believe that a candidate is an unsuitable appointment to his or her particular position and may, even unconsciously, give incomplete, slanted or exaggerated information as a result.

24. In addition, when dealing with information provided by candidates or referees, the NZSIS must:

    24.1. *Rely on objective factual investigation, not personal impressions:* The NZSIS may not use the demeanour of a candidate or referee as a sole or conclusive indication of that person's credibility or of the reliability or unreliability of particular information that that person provides.

    24.2. *Assess the reliability of particular information, not the apparent character of the candidate or referee who provides it*: NZSIS must ensure that it assesses the reliability of each relevant statement, rather than attempting to assess and rely upon the character of the source, so as to avoid the "halo effect":[9]

---

8 See below at paragraphs 34ff.

9 *R v Munro* [2008] 2 NZLR 87 (CA(FC)) [76] & [80]-[81] (citations omitted) and see also (in the particular context of security vetting) above n 6.

> "Studies have also highlighted the fact that witnesses who appear confident and open, and have a good memory for peripheral detail, are far more likely to be believed, regardless of whether they are truthful. Unsavoury and unattractive witnesses are less likely to be believed, because there is a general bias in favour of believing that attractive people are honest. Similarly, once a positive or negative impression is formed, this will attach to all of that witness' evidence. People do not tend to differentiate between 'parts' of a witness' testimony. This has been described as the 'halo effect' whereby one perceived good or bad quality in a person will tend to colour all judgements pertaining to the person."

24.3. *Make an objective evidence-based assessment of the reliability of information provided:* NZSIS may not assume a referee to be biased – whether positively or negatively – simply because of some fact about their relationship to, or history with, the candidate. What is required is objective factual investigation of the reliability of that person's statements, including through checking and corroboration.

Disclosure to the candidate for response

25. If an adverse or qualified assessment is in prospect, the candidate must be given the opportunity to know and answer the case against him or her before the NZSIS reaches a concluded view. In such instances, NZSIS must first:

    25.1. Tell the candidate of the proposed adverse or qualified conclusion(s);

    25.2. Give the candidate the information and inferences relied upon to support that proposed conclusion, as well as any contradictory information or inferences, and the way in which the information and/or inferences are considered relevant to identifiable security vulnerabilities.[10] Information may be withheld only if and to the extent that, it falls within one of the exceptions noted in the next section; and

    25.3. Give the candidate an adequate opportunity to respond, including explaining that the candidate may:

    - respond within a reasonable time period, if he or she does not wish to or is unable to respond immediately;
    - provide further information or ask an employer or other relevant agency to provide further information;
    - respond through a lawyer or other representative; and
    - respond through or with the assistance of his or her own expert, where issues of expert judgement arise.

Engagement with responses, including further information-gathering as needed

26. NZSIS must consider the response(s) provided carefully and with an open mind. In practice, that will require:

    26.1. Pursuit of any further lines of inquiry that may be prompted by the candidate's response. Where a candidate raises points of expert judgement or legal objections, that will in general require NZSIS to seek expert and/or legal assistance, as addressed in the next section. If those efforts produce further information or inferences relevant to a proposed adverse or qualified conclusion, the candidate must be told of those and given further opportunity to respond; and

    26.2. Consideration of the candidate's response(s) and any further information or inferences that arise from further investigation as part of the overall assessment. The NZSIS's ultimate assessment should explain whether and why NZSIS has accepted or rejected the particular response(s) given.

[10] The NZSIS could adopt the Australian practice of providing a written draft of the proposed adverse or qualified recommendation and supporting information and reasoning to the candidate.

Exceptions to obligations of disclosure

27. The obligation of disclosure is subject to specific, narrow exceptions. Adverse allegations or information need not be disclosed to the candidate if:

    27.1. Disclosure would give rise to at least "a distinct and significant possibility" of damage to security or intelligence operations, foreign relations or other protected interests; or

    27.2. Disclosure would be likely to endanger a person; or

    27.3. Non-disclosure is necessary to protect a statement of opinion made by a referee following an assurance of confidence from NZSIS. Factual statements by referees are not in general protected from disclosure;[11]

28. A further, narrow, exception is discussed at paragraphs 34-38 below.

Application of exceptions

29. The standard of whether non-disclosure is necessary to safeguard national security or other protected interests is stringent: there must be a significant possibility of some particular damage to protected interests.[12]

30. It is also not permissible to withhold information where disclosure is seen to be difficult, inconvenient or simply unnecessary. For example, non-disclosure of adverse information would not be justified simply because the Service may believe that the relevant allegations are already known to the candidate, that they are unanswerable or that putting adverse information for response would be personally difficult or embarrassing for candidates or for the interviewing officer.

31. Further, there is no basis for non-disclosure so far as some or all of the adverse information can be safely disclosed; some or all information has been disclosed already; or where the information can or must be disclosed, for example:

    31.1. Where the candidate is independently entitled to the information, as with health practitioners' assessments;[13]

---

11 Privacy Act s 29(3): evaluative or opinion material must be compiled "solely" for the relevant purpose and see, further, G Taylor & R Taylor *Judicial Review: A New Zealand Perspective* (3ed, 2014) 341 ("parts of the material which are not assessing the subject or expressing opinion, but rather stating the facts on which assessment or opinion is based will not be protected"); though cf *Privacy Law and Practice* at ¶PVA29.9.

12 *Commissioner of Police v Ombudsmen* [1988] 1 NZLR 385 (CA); and see also the requirement of specific identification of the risk in *Choudry v Attorney-General (No 2)* [1999] 2 NZLR 582 (CA), 596-597.

13 Health Act 1956, s 22F; *McInerney v MacDonald* [1992] 2 SCR 138; *R (ex p Martin) v Mid-Glamorgan Family Health Services Authority* [1995] 1 WLR 110, 119; *Hannover Life v Sayseng* [2005] NSWCA 214. The statutory rights to information are expressed to be subject to Privacy Act exceptions, including the referee exception discussed below, but it is unlikely that a health practitioner can provide an expert opinion on condition of non-disclosure, whether for ethical reasons or because there is no proper reason to require an expert professional assessment to be given in confidence, or, at least, that the Service could rely upon such an opinion: see, for example, *Hannover* (natural justice requires opinion provided to third party to be provided to patient).

31.2. Where the information need not have been obtained in confidence, for example where a referee or other person is in fact willing or obliged to provide the information on an attributable basis; or

31.3. Where the relevant information can be safely disclosed in unattributable form, for example where sensitivity relates only to the identity of a source and that source is not evident from the information itself or, failing that, where information provided in confidence can instead be obtained for attribution or from a non-sensitive record, such as an employment file.[14]

Obligations where any information withheld

Adequacy of summary/"gist"

32. Where information cannot be disclosed in full, a summary or redacted version must be provided to the fullest extent possible. The broad test is whether or not the substance and detail of the adverse allegation or information, including corroborating or contradictory information and any information going to the credibility of that adverse material, has been provided in sufficient detail that the candidate can respond to it fully.[15]

Particular duty of "utmost good faith"

33. Where the Service seeks to rely upon adverse information that it cannot disclose to the candidate, it has a particular duty of candour and utmost good faith that requires:[16]

33.1. A particularly thorough approach to ensure the accuracy, currency and comprehensiveness of that information; and

33.2. The NZSIS record of decision must set out an even-handed assessment of all information, both positive and adverse, so as to compensate as far as possible for the candidate's inability to raise responses, additional information or doubts.

---

14 See, for example, *Mohamed, R (on the application of) v Foreign Secretary* [2011] QB 218 (EWCA), [59] (respondent's claim to non-disclosure of security information rejected where relevant information available from public sources).

15 *Home Secretary v AF (No 3)* [2010] 2 AC 269, [59]: "sufficient information to enable [the candidate] actually to refute, in so far as that is possible, the case made out against [him or her] …"**.** This requirement is not absolute and may be limited in a truly exceptional case, but in such cases additional safeguards then apply: see *Tariq*, above n 2, [69], and the following section.

16 See *Canada v Harkat* [2014] 2 SCR 33, [101]-[103], relevant information is to be "complete and thorough" and, adopting *Re Almrei* [2011] 1 FCR 163 "the party relying upon the presentation of *ex parte* evidence will conduct a thorough review of the information in its possession and make representations based on all of the information including that which is unfavourable to their case" and finding a duty of candour and utmost good faith, including taking reasonable steps to ensure currency and accuracy.

Exceptional cases where adequate disclosure cannot occur

34. The approach set out in this review will apply to the vast majority of NZSIS security vetting assessments.

35. However, it is possible that, in an exceptional case, the nature of some particular information or of its source means that it is not possible to provide adequate disclosure of adverse information in the way described in the previous section.

36. Cases falling within this second exception will be truly rare; it has not arisen in any of my office's inquiries to date.[17] However, such a case did arise in the United Kingdom Supreme Court decision in *Tariq*, in which particular intelligence information relied upon by vetting officers was so sensitive that sufficiently detailed information could not be provided to the candidate.[18]

37. In such instances, the NZSIS is subject to additional and stringent obligations.[19] It must:

    37.1. So far as possible, corroborate the particular adverse information;

    37.2. Take all relevant steps to determine that the information is reliable, current and comprehensive; and

    37.3. In deciding whether to take account of the particular information, weigh up both the gravity of that adverse information in terms of national security and the risk that the information may in fact be unreliable or might have been rebutted or explained, but for the non-disclosure.[20]

38. A situation such as this would be exceptional and pose difficult issues: specific legal advice should be sought in any such case.

---

17 In *Tariq*, above n 2, it was suggested by some members of the Court (see, for example, [72]) that information and methods relevant to security vetting in the United Kingdom "usually, if not invariably, require" secrecy and confidential sources, whose safety may otherwise be at risk. In New Zealand, the criteria for security vetting are set out in the published *Protective Security Requirements* (see above n 2) and most of the relevant information identified there is not of that kind.

18 *Tariq* above n 2.

19 The standard that NZSIS must meet in dealing with such a case is still higher than in *Tarig*: in accepting the non-disclosure in that case, the United Kingdom Supreme Court took account of the various additional protections provided in United Kingdom law for candidates in such cases, as set out at paragraph 50 below, but not available in New Zealand.

20 *VEAL v Minister for Immigration and Multicultural and Indigenous Affairs* (2005) 225 CLR 88, [23]-[29].

Candidates' responses involving matters of expert judgement

39. If a candidate's response includes information from an expert, such as a letter or opinion from a doctor or other qualified person or records compiled by such a person, NZSIS must ensure that it takes the steps necessary to engage with that information, as follows.

40. If the NZSIS has not already obtained such opinion or advice:

    40.1. NZSIS must obtain its own expert opinion or advice to assess the relevance and significance of that expert information, following the approach outlined in paragraphs 18-19 above.

    40.2. If the opinion or advice then obtained by NZSIS contradicts the candidate's expert information and tends to support or not contradict NZSIS's proposed adverse or qualified findings, NZSIS must disclose that opinion or advice to the candidate and provide an opportunity for response, in line with paragraphs 25.2 and 25.3 above.

41. If the NZSIS has already obtained expert opinion or advice and the candidate's expert information contradicts or doubts that opinion or advice or the candidate's expert information raises matters not covered by that opinion or advice:

    41.1. NZSIS must decide whether simply to accept the candidate's response, if for instance the candidate's expert information adequately addresses the basis for its concern.

    41.2. If NZSIS does not simply accept the candidate's response, it should provide the response to the expert that NZSIS had consulted (or, if unavailable or no longer appropriate,[21] another expert) for his or her assessment.

42. If, following these steps, the opinion, advice or information provided by the respective experts is consistent, then the NZSIS can act on that. If, however, NZSIS is faced with one or more contradictions – for example, if two clinicians reached different views on the existence, character and/or consequences of a mental health condition – then NZSIS must choose between each of the relevant conclusions reached by each expert, taking into account:

    42.1. The respective clinical or other expertise of each expert;

    42.2. The extent to which each has engaged with the factual information that underpins their respective views; and

    42.3. The persuasiveness of the experts' explanations of their conclusions and the connection between those conclusions and any security concern.

43. If, in any case, NZSIS considers that the candidate's expert information is incomplete or not directly relevant, for example because it does not address security criteria or vulnerabilities, it is appropriate to advise the candidate of any such any apparent omission and provide a further opportunity to address that omission, so as to ensure that NZSIS has the fullest information available.

---

[21] For instance, NZSIS might have initially consulted a counsellor or psychologist over a mental health issue. However, if the candidate's expert information were to include a psychiatrist's records or opinion, it will be necessary to seek psychiatric opinion in response.

Recorded decisions, including reasons

44. NZSIS vetting officers must record the specific reasoning followed in making their assessment.

    The record can be short but must include:

    44.1. The information compiled, including acknowledgement of any relevant information that could not be obtained;

    44.2. The steps taken to assess the reliability, currency and comprehensiveness of that information and an explanation of any information not taken into account;

    44.3. In any potential adverse or qualified case, the information, allegations and inferences disclosed to the candidate; any information or allegations withheld and the basis for doing so; the candidate's response(s) to the disclosed information; and any further investigative steps taken as a result; and

    44.4. A reasoned assessment of all the factual information against the applicable criteria.

45. The need for such a record arises for several reasons:

    45.1. Assessments have grave consequences both for national security and for the individuals concerned;

    45.2. Assessments are a collective effort, with an initial recommendation made by one or more NZSIS officers subject to approval and, on occasion, alteration by others. Adverse recommendations are ultimately approved by the Director. Clear reasoning is necessary to allow those responsible for approval to provide a meaningful check and to record where approval is not given or where recommendations are altered through the process;

    45.3. Procedural fairness requires the Service to disclose its adverse inferences and the basis for those inferences to the candidate for response, and then to take the response into account. That cannot occur if a reasoned analysis is not prepared;

    45.4. NZSIS vetting officers are required to make a considered and balanced assessment of complex information against decision-making criteria. These officers make initial recommendations and deal with numerous decisions each year. It is not practically possible to rely upon officers' own recollections of their reasoning;

    45.5. Records serve as a safeguard against error for vetting staff and for those responsible for approving recommendations, ensuring that decision-making criteria are clearly applied and any risk of unconscious bias is minimised. If an assessment is found to have been mistaken, records provide some means of establishing how the mistake occurred;[22] and

    45.6. There is a legal risk that, where reasoning is not recorded or recorded only in broad or contradictory terms, it may be inferred that reasoning simply did not occur at all.[23]

---

22 See, also, Australian Government *Personnel Security Guidelines: Vetting Practices* [7.2], above n 7, 57.

23 See, for example, *Chief Executive of the Department of Labour v Taito* [2006] NZAR 420 (CA), [24]; *Bovaird v J* [2008] NZAR 667 (CA), [68].

Appendix: Comparable overseas practice

46. In compiling this summary, and undertaking the inquiries on which it is based, we took into account not only relevant law, much of it drawn from the United Kingdom and Canada, but also comparable practice in those countries and also in Australia and the United States, as all four operate similar security vetting programmes. The following summary outlines the approach taken in those jurisdictions.

47. ***Australia***: the clearance subject has a right to:[24]

> Be told the case to be met (for example, that an agency is considering denying or withdrawing a clearance, or imposing conditions on the clearance), including reasons for this proposal and any negative or prejudicial information relating to the clearance subject, to the fullest extent possible consistent with national security, that is to be used in the clearance process. The case to be met could be a letter or a draft report, or it could be a summary of the issues being considered by the assessing officer/Delegate. …
>
> A real chance to reply to the case to be met, whether that is in writing or orally.

48. ***Canada***: when consideration is given to denial or revocation of a clearance, the candidate is to be informed in writing, provided with reasons except so far as those reasons cannot be disclosed under the Privacy Act, and given the opportunity to validate or refute adverse information.[25]

49. ***United States*** (taking the Department of Defense as an example): a final unfavourable clearance decision not to be made without notice of specific reasons, opportunity to respond to those reasons, provision of a hearing and a right to cross-examine those providing adverse information and opportunity to present contrary evidence. Similarly, the standard *Adjudicative Desk Reference* outlines that candidates, in the case of an adverse or qualified recommendation, should be provided with a comprehensive explanation of the basis for the recommendation, any documents, records or reports upon which the recommendation was based, an opportunity to respond and the assessor must then address that response.[26]

50. ***United Kingdom***: The *HMG Personnel Security Controls* do not contain similar detail to that found in the other Five Eyes governments' procedures, but do refer to "disclosure to the [candidate]"; state that a candidate should, where possible, be given reasons; and also state that internal and external review procedures for existing employees should be as "[transparent] as possible, within the bounds of national security and third party confidentiality". There is also provision in the *Controls* for an Appeals Panel and for the appointment of a special advocate in any consequent employment proceeding.[27]

---

24 *Personnel Security Procedural Fairness Guidelines*, p 2 and Australian Government *Personnel Security Guidelines: Vetting Practices* [6.1]-[6.2], pp 54-56.

25 *Standard on Security Screening*, Appendix D, 2

26 *Directive 5220.6: Defense Industrial Personnel Security Clearance Review Program* [4.3] and above n 6, 483. United States caselaw is limited, and substantive review of decisions is also constrained by the wider United States executive/agency deference doctrines (see, for example, *Department of the Navy v Egan* 484 US 518 (1988)), which have no application in New Zealand.

27 *HMG Personnel Security Controls* pp 12, [46] & [47]; p 13, [50].