Te Pourewa Mātaki
Inspector-General of Intelligence and Security

Review of NZSIS Use and Sharing of Vetting Information

Public Report

Brendan Horsley

Inspector-General of Intelligence & Security

October 2023

Contents

SUMMARY

1. I have reviewed the New Zealand Security Intelligence Service (NZSIS) systems for compliance with section 220 of the Intelligence and Security 2017 (ISA), which puts limits on the use of security clearance assessment ("vetting") information. This public report is derived from my classified report. The classified report has greater detail about some incidents and internal NZSIS policies and procedures. However, that has no material effect on the substance of this public report or my recommendations.

2. Section 220 allows information obtained by or disclosed to the NZSIS for a security clearance assessment to be used only for that assessment, another security clearance assessment, or counter-intelligence.[1] In my view, s 220 prohibits access to, disclosure of, and use of vetting information for purposes outside those listed in the Act.

3. My review found inconsistencies in how the NZSIS interprets and applies s 220 when carrying out its functions. At times this has resulted in a lack of compliance with the ISA.

4. I have identified three alternative purposes for which the NZSIS has, on a few occasions, accessed and used or disclosed vetting information, or sought to do so:

   - counter-terrorism investigations,
   - sharing with law enforcement, and
   - internal disciplinary purposes.

   I consider these were contrary to s 220. None were permissible, in my view.

5. Most instances have involved the NZSIS seeking and being granted intelligence warrants to access vetting information for counter-terrorism purposes. In my view a warrant may not authorise activities which are unlawful under the ISA itself.

6. I recommend the NZSIS cease applying for intelligence warrants to access vetting information contrary to s 220 and revoke any related internal policies.

7. I also recommend the development of further guidance for NZSIS staff to ensure compliance with s 220.

---

1 ISA, s 220(1).

INTRODUCTION

Background

8. Under the Intelligence and Security Act 2017 (ISA) the functions of the New Zealand Security Intelligence Service (NZSIS) include protective security services, advice and assistance.[2] This function includes conducting security clearance assessments (vetting). Individuals who are required to access classified information, assets (such as a Defence Force aircraft or ships) or work locations need a national security clearance.[3] The assessment of an individual's suitability to hold a security clearance is necessary to protect classified information, resources, and systems.[4]

9. The use of security clearance assessment information is controlled by s 220 ISA. In short such information may only be used for vetting purposes or for "counter-intelligence", which is defined in the Act.[5]

10. On rare occasion the NZSIS has used or disclosed vetting information for other purposes. In most cases this prompted questions from my office and responses from NZSIS.[6] This review surveyed and analysed the issues that have arisen with the interpretation and application of s 220 to draw overarching conclusions.

Review scope and criteria

11. This was a review under section 158(1)(f) ISA. The review considered:

    - what s 220 requires,
    - how the NZSIS has responded to issues in the interpretation and application of s 220, and
    - whether the NZSIS's approach, including relevant policies and practices, has enabled it to respond lawfully and properly.

12. As the NZSIS's approach to compliance with s 220 has included seeking warrants authorising use of vetting information contrary to the section, I have also reviewed under s 158(1)(i) the issue and execution of those warrants.

---

2 ISA, s 11(3)(a)(i).

3 Protective Security Requirements *Getting a national security clearance* (August 2022) at 2.

4 The candidate's organisation decides if their role requires a national security clearance and refers the candidate to NZSIS for a security clearance assessment. The NZSIS makes a recommendation based on its assessment. The organisation makes the final decision on granting the security clearance.

5 ISA, s 220(3).

6 The IGIS has investigated complaints and privacy breaches relating to the use and sharing of security clearance information. For reviews on related issues see: Cheryl Gwyn (IGIS) *Review of NZSIS holding and use of, and access to, information collected for security vetting purposes (Part One)* (4 April 2016); Brendan Horsley (IGIS) *Review of NZSIS framework for disclosing incidentally obtained information on potential criminal offending to the Police* (30 July 2021). See also *Office of the Inspector-General of Intelligence and Security: Annual Report for the year 1 July 2020 to 20 June 2021* (11 November 2021) at 5.

SECTION 220 OF THE INTELLIGENCE AND SECURITY ACT 2017

13. Section 220(1) ISA states that the only purposes for which security clearance assessment information may be used are:

    (a) the security clearance assessment:

    (b) any other security clearance assessment:

    (c) counter-intelligence.

14. Section 220(3) defines a security clearance assessment as:

> an assessment conducted by the New Zealand Security Intelligence Service in the performance of its function under section 11 for the purpose of making a recommendation as to an individual's suitability to hold a New Zealand Government-sponsored national security clearance.

15. "Counter-intelligence", for the purposes of s 220, is defined in s 220(3) as

> the intelligence activities carried out to identify and counteract the threat, or potential threat, of unauthorised disclosure of official information by a person who holds, or has held, a New Zealand government-sponsored national security clearance.

16. Section 220(2) states that s 220(1) applies despite anything in Information Privacy Principle 10 (IPP 10) set out in s 22 of the Privacy Act 2020. IPP 10 puts limits on the use of personal information but allows an intelligence and security agency to use personal information collected for one purpose, for another purpose. Section 220(2) therefore rules out any use of security clearance assessment information by the NZSIS for any purpose other than those permitted under s 220.

17. In 2016, before the Security and Intelligence Bill was introduced to the House, the Inspector-General of Intelligence and Security (IGIS) reported on a review of NZSIS holding and use of, and access to, information collected for security vetting purposes.[7] In that report the IGIS noted that security clearance assessment records "likely comprise the most sensitive repository of such personal information held by the New Zealand government"[8] and the NZSIS had enabled access to them for various purposes.[9] The IGIS's criticism in the report is believed to have informed the strict wording of s 220.

18. The underlying policy of s 220 is to ensure confidentiality in the vetting process, to ensure that applicants for security clearances are candid and thorough in their responses. Effective vetting is underpinned by the ability of NZSIS to encourage candidates to disclose relevant matters that are highly sensitive and personal (such as drug use, criminal offending, financial difficulties), about themselves, relatives and friends. Such disclosures are sought on the basis of assurance that the information will not (subject to the limited exceptions in s 220) be used or shared for any purpose other than vetting.

---

7 Cheryl Gwyn (IGIS) *Review of NZSIS holding and use of, and access to, information collected for security vetting purposes (Part One)* (4 April 2016).

8 Above n 7 at [2].

9 Above n 7 at [38].

19. As I understand it, the apparent rationale for the counter-intelligence exception in s 220 is that because a cleared person will have access to national security classified information, any indication that they might disclose any official information (whether national security classified or not) without authorisation is grounds for concern that they might put national security information at risk. Any such risk is a valid matter for NZSIS, with its protective security function, to investigate. As vetting information is collected for the purpose of protecting national security classified information, accessing vetting information for a counter-intelligence investigation is consistent with the purpose for which vetting information is acquired.

NZSIS POLICY AND PROCESS

20. The section 220 safeguards are reiterated in multiple NZSIS policies and procedures, from vetting to counter-intelligence operational policies. The policies and procedures summarised here are the main documents relevant to this review.

NZSIS policy for using security clearance information for counter intelligence activities

21. This policy sets out NZSIS's definition of counter-intelligence, which is based on s 220(3), and identifies responsibilities for counter-intelligence activities involving vetting information.

22. The policy only covers the use of security clearance information for NZSIS counter-intelligence investigations. No guidance is provided on sharing security clearance assessment information with other agencies for counter-intelligence purposes.

23. The policy also outlines the different access controls on different levels of vetting information for counter-intelligence.

24. The policy details the process for granting access and the purposes for which the information may be used. Access to vetting information is tightly controlled including for counter-intelligence activities. The Security Vetting Unit Manager identifies the relevant information for counter-intelligence which must then be approved by a senior staff member before being released to Counter-Intelligence staff.

NZSIS Standard Operating Procedure relating to sharing vetting information within NZSIS

25. This SOP is a step-by-step guide to sharing security clearance assessment information on NZSIS systems. The SOP covers sharing vetting information for security clearance assessments or counter-intelligence.

26. As the title suggests, the SOP only applies to the disclosure of security clearance assessment information *within* NZSIS and the guidance provided does not extend to information-sharing with other agencies.

27. The SOP outlines the approval process for:

    - if a Vetting Officer conducting a clearance assessment believes information should be disclosed for a counter-intelligence or insider threat investigations, and

- if Insider Investigations staff request security clearance assessment information about a candidate or a referee for a counter-intelligence purpose.

28. The SOP states that vetting information will only be disclosed when directly relevant to a counter-intelligence activity. The approver must be satisfied that the disclosure is lawful, necessary and proportionate.

NZSIS Standard Operating Procedure relating to accessing vetting information under an intelligence warrant

29. This SOP presumes the NZSIS may be granted an intelligence warrant to access and use security clearance assessment information for purposes outside of those listed in s 220 ISA.

30. The SOP outlines the approval process for requests from investigating officers to access vetting information under warrant. The approver must take into account a number of things such as necessity and proportionality.

NZSIS Standard Operating Procedure relating to quality assessments for vetting

31. This SOP is for quality control checks on the conduct of vetting cases.

32. When conducting quality controls the senior vetting staff member or manager assesses all completed security clearance assessment records on the different vetting systems. Generally senior vetting staff are not required to look at candidates' personal information for quality assessments. Listening to the recordings of vetting interviews is not part of the quality control check. The only exception to this procedure is for new staff where 100% of their cases undergo quality assessment.

Your Interview Guide

33. Vetting candidates are provided with a range of information on the process and what is expected of them, including *Your Interview Guide*.

34. Candidates are encouraged to be completely open and honest in their responses throughout the assessment process, including when the information provided may reflect negatively on them or someone they know. Candidates are also advised they may lose or be denied a security clearance if they are found to be deliberately withholding information.[10]

35. The interview guide states that:

> your personal information, including the audio file of your interview, will only be accessible to the vetting staff involved in your vetting assessment. There are strict controls on access to this file and strict legal limits on its use.

36. The interview guide also refers candidates to the Protective Security Requirements (PSR) website for more information on what NZSIS looks into, and the candidate's legal rights and

[10] NZSIS *Your Interview Guide* (Updated July 2021).

responsibilities. The PSR guide for candidates *Getting a National Security Clearance* provides similar details on the controls on use of security clearance assessment information:[11]

> all information obtained during the course of the vetting process is kept in NZSIS vetting records. The information NZSIS collects is not made available to government organisations, except so far as necessary to support recommendations on the clearance to the originating organisation's Chief Executive.

[11] Protective Security Requirements. *Getting a National Security Clearance: A candidate's overview of the national security clearance vetting process* (December 2019).

EXAMPLES AND ANALYSIS OF NZSIS USE AND SHARING OF SECURITY CLEARANCE ASSESSMENT INFORMATION

37. On a limited number of occasions, since the enactment of s 220, the NZSIS has used security clearance assessment information for purposes other than vetting or counter-intelligence and sought authorisation to access security clearance assessment information for purposes other than vetting or counter-intelligence.

38. This review identified three themes:

Figure 1: Examples of where NZSIS has used and shared security clearance assessment information for purposes outside of Section 220 ISA

Counter-terrorism purposes

Person of national security interest under counter-terrorism investigation

39. In mid-March 2019, the NZSIS identified an individual as a person of national security interest (Person 1) under a counter-terrorism investigation.

40. An intelligence analyst sought the Director of Security's[12] approval to conduct a range of specified checks on Person 1, copying in the counter-terrorism investigation group email. Although the intelligence analyst did not request access to security clearance assessment information, the Director of Security replied that he had already approved access to any vetting information held by NZSIS on Person 1 for the purposes of a counter-intelligence investigation. The Director of Security referred the request to the Director of Intelligence for approval of "investigative and operational activity" noting that this was not an insider threat case. The Director of Intelligence

[12] This role is now Deputy Director-General Protective Security (DDGPS).

responded with "approved". His email did not specify what activities were approved, however the Director of Intelligence recalls he was approving the other investigative activities requested in the analyst's email and not the access to vetting records. The Director of Security later told the IGIS he understood the counter-terrorism team wanted access to the vetting records. The intelligence analyst's request was made in the days immediately following the Christchurch terrorist attacks, during which NZSIS staff and managers were investigating and managing large volumes of material.

41. The intelligence analyst reviewed Person 1's vetting file, presumably on the assumption that access and use had been approved by either or both Directors. Information from the vetting records considered relevant to the counter-terrorism investigation was then shared with other staff working on that investigation.

Accessing vetting records under intelligence warrants

42. In early 2019 the NZSIS applied for a class warrant to authorise activities for counter-terrorism investigations. Among other things the NZSIS sought authorisation to "search and seize security clearance assessment information" of all individuals within the target class.

43. The warrant was issued by the Minister and the Commissioner of Intelligence Warrants as sought.

44. Ultimately nobody was targeted under the warrant, so no vetting information was accessed or used. The following year, the warrant was renewed without the search and seizure of vetting information as an authorised activity.

45. Also in early 2019, the NZSIS applied for an amendment to a different class warrant to collect against domestic counter-terrorism threats. The amendment included seeking authorisation to "search and seize security clearance assessment information" for the target class. As part of the case for this NZSIS cited two examples of "targets or potential targets" who were security clearance holders at the time.

46. The first person became the target of an individual warrant, which did not authorise seizure of vetting information. The second person was determined to have been incorrectly identified as a target. As far as NZSIS is aware, no vetting information was accessed under the amended warrant.

47. In late 2019, the NZSIS applied for an intelligence warrant to collect against an individual (Person 2) assessed as posing a counter-intelligence and a domestic terrorist threat.

48. NZSIS sought authorisation to (among other things) search and seize Person 2's vetting information. In the intelligence warrant application NZSIS stated it could lawfully access vetting records for counter-intelligence activities, but NZSIS sought a warrant so that it could use any relevant information for the counter-terrorism investigation.

49. The warrant application also set out the possible scope of the proposed access to vetting information, which included listening to the audio recording of the vetting interview and reviewing any associated documents. The NZSIS anticipated these activities would enable it to obtain information that Person 2 had not disclosed to close associates, such as lifestyle, personal choices, criminal activity, political affiliation, drug use and sexual encounters. NZSIS also stated it was

possible that the information could include that provided from referees or other third parties such as the Police.

50. The warrant was issued by the Minister and Commissioner of Intelligence Warrants as sought.

51. No counter-terrorism investigators accessed Person 2's vetting information under this warrant.

Can the NZSIS access and use vetting information for another purpose without an intelligence warrant?

52. When the NZSIS accessed the vetting records of Person 1 it did not have an intelligence warrant authorising it to do so. It appears that Person 1's vetting records were initially accessed by Insider Investigations for a counter-intelligence investigation, which is permitted under s 220. But there were no records that identified Person 1 as a possible threat to the security of official information. Further, the subsequent sharing of that information was for a counter-terrorism investigation. Counter-terrorism is not a permitted use of vetting information. Accessing Person 1's records for that purpose was a clear breach of s 220 and no manager had authority to approve it. I would have expected staff members at the Director level to have been better across the issue and their responsibilities under s 220.

53. After s 220 was enacted NZSIS considered whether *accessing* vetting information could be distinguished from *using* it, so that it could be accessed for general intelligence purposes without breaching s 220. It concluded that accessing the information would invariably lead to using it. The access and use of Person 1's vetting information was inconsistent with this advice at the time because the vetting records were shared on the basis that the counter-terrorism investigation would use that information. This demonstrates the difficulties in separating *access* from *use.* NZSIS's position on s 220 was revisited in January 2019, as discussed later in this report.

Can an intelligence warrant override section 220?

54. The obtaining of intelligence warrants raises the question of whether those warrants can authorise access and use of vetting information despite the limits contained in s 220.

55. The legal framework for authorisations, which includes intelligence warrants, is set out in Part 4 ISA. Section 49 states that:

> (1) an intelligence and security agency may carry out an otherwise unlawful activity only if that activity is an authorised activity…
>
> (3) an authorised activity may lawfully be carried out by an intelligence and security agency despite anything to the contrary in any other enactment.

56. NZSIS's view is that accessing and using vetting information outside the parameters of s 220 would ordinarily be unlawful, but if a warrant authorises access to vetting information for other purposes then such access and use id lawful under s 49.

57. The previous IGIS Cheryl Gwyn expressed some concern regarding the use of warrants to search and seize vetting information for purposes other than those permitted under s 220, noting that the threshold for such a warrant would always be "especially high" given the restrictive policy

behind s 220. She did not however reach a settled view on the matter.[13] I have come to a stronger conclusion on this point.

58. I do not consider a warrant can lawfully authorise the access and use of vetting information for purposes outside of s 220. Section 49(3) ISA provides that an authorised activity may lawfully be carried out "despite anything to the contrary *in any other enactment*" [my emphasis]. In my view, if the intent of Parliament was to enable an authorisation to override anything in the ISA itself, the section would state '*in this or* any other enactment', or words to that effect. Alternatively access to vetting information under warrant might have been included in the exceptions within s 220 itself.

59. If a warrant could authorise activities otherwise prohibited by s 220 that would imply other safeguards in the Act could be similarly bypassed by authorisation, which would defeat the purpose of enacting them. I note that the Reviewers of the Intelligence and Security Act 2017 reached the same view, that "activities that are unlawful under the ISA itself cannot be authorised".[14]

60. The third intelligence warrant (discussed at [47]) raises the same issue as the other intelligence warrants but in a different context: can the NZSIS access and use vetting information for counter-intelligence purposes, then use that information for counter-terrorism purposes if authorised to do so? I accept that NZSIS can have grounds to run both a counter-intelligence and a counter-terrorism investigation simultaneously against the same individual. But s 220 means that vetting information can only be accessed for the former. In my view that is simply a consequence of the strict conditions s 220 applies.

61. If an intelligence warrant cannot authorise access to vetting information contrary to s 220 it follows that the NZSIS standard operating procedure on accessing vetting information under an intelligence warrant has no valid purpose.

62. **Recommendation 1:** I recommend NZSIS cease applying for intelligence warrants to access security clearance assessment information and revoke the Standard Operating Procedure on accessing vetting information under an intelligence warrant.

Law enforcement purposes

Report of possible criminal offending to New Zealand Police

63. In 2020 a vetting candidate disclosed to NZSIS during their vetting interview information about possible serious criminal offending.[15] After seeking advice from NZSIS Legal and approval from the Director-General and the Director of Security, the NZSIS disclosed that information to the New Zealand Police in late 2020.

---

13 Letter from Cheryl Gwyn (IGIS) to Rebecca Kitteridge (Director-General NZSIS) regarding Amendment to warrant (15 April 2019).

14 Hon Sir Terence Arnold KNZM KC and Matanuku Mahuika (2023) *Taumaru: Protecting Aotearoa New Zealand as a free, open, and democratic society*. Wellington: Ministry of Justice. At [6.13].

15 Brendan Horsley (IGIS) *Annual Report 2020-2021* (11 November 2011).

Can the NZSIS disclose vetting information to the New Zealand Police?

64. When deliberating whether to share the information about the possible criminal offending, the NZSIS came to the view that s 220 prohibits the *use* of security clearance assessment information, but not the *disclosure* of that information. My understanding is that the rationale for disclosing the information was due to the seriousness of the crime, the possibility of harm to others, and that the disclosure was made shortly after receiving the information.

65. The Privacy Act 2020 distinguishes between *use* and *disclosure* in Information Privacy Principles (IPP) 10 and 11 respectively. IPP 11 puts limits on the disclosure of personal information except in the following circumstances:

> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment for offences…
>
> (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.[16]

66. In the NZSIS's view s 220 does not override IPP 11 NZSIS concluded that s 220 regulates the *use* of vetting information but not the *disclosure* of vetting information. The NZSIS concluded it could disclose the personal information under IPP 11 to perform its function of providing advice and assistance to the New Zealand Police.[17]

67. I was notified at the time of the NZSIS's intention to disclose the vetting information to the Police. I advised NZSIS that in my opinion any such disclosure may be unlawful and that if the Director-General disagreed she should obtain advice from Crown Law before disclosing anything to Police.

68. I considered the proposed distinction between *use* and *disclosure* was entirely academic. The NZSIS's intention on sharing that information was so that it could be *used* in a criminal investigation. In short, I was not convinced by the NZSIS's reasoning and I considered the disclosure a breach of s 220.

69. The NZSIS sought advice from Crown Law. The practical consequence of that legal advice was that NZSIS could not disclose vetting information to another agency unless that agency was going to use it to assist with a security clearance assessment or for counter-intelligence.

70. NZSIS subsequently asked Police to destroy or return the information. I understand that as far as NZSIS is aware Police took no action on the information beyond initial checks against other information it already held.

71. I maintain my view that the disclosure to the Police was unlawful. If there is no meaningful distinction between disclosure and use then NZSIS simply cannot disclose vetting information to the Police unless for the purposes in s 220. It is possible that the NZSIS could be faced with the situation of a vetting candidate disclosing information about criminal activities involving imminent serious harm. Whilst this would be a difficult prospect, I consider sharing information with Police

---

[16] Privacy Act 2020, s 11(g).

[17] ISA, s 13(1)(b) ISA.

in such circumstances might be morally defensible but it still would be unlawful and potentially an offence.[18]

72. Many of NZSIS's policies and procedures could provide clearer guidance to staff on the practicalities of the strict wording of s 220. Current NZSIS policy and procedure only provides guidance on sharing information with counter-intelligence investigations and insider threat investigations *within* NZSIS. This means there is no formal guidance for staff on the very limited scope for disclosing vetting information to other agencies. Filling this procedural gap would likely be useful for NZSIS staff who have a legitimate basis for sharing vetting information with other agencies for counter-intelligence or security clearance assessments. Any updates to procedural guidance should clearly outline what is *not* permitted under s 220 to avoid any confusion or over-extension of s 220's purpose. Any relevant training should include examples of situations that might plausibly arise but where sharing that information would not be permitted.

73. **Recommendation 2:** I recommend NZSIS updates and promulgates the relevant internal policies and procedures including:

- updates to the Policy regarding using vetting information for counter-intelligence activities and the Standard Operating Procedure on sharing vetting information within NZSIS to provide guidance on when sharing vetting information is and is not permitted, and
- the development of a Standard Operating Procedure on sharing security clearance assessment information with other agencies.

Disciplinary purposes

Investigation into a complaint regarding a Vetting Officer's conduct

74. A vetting candidate made a complaint in 2019 to the NZSIS that during their interview the Vetting Officer used inappropriate phrasing, intrusive questioning, and revealed sensitive and personal information about another clearance holder. As part of the investigation into the complaint, the Security Vetting Unit Manager at the time listened to five vetting interview recordings.

75. In the disciplinary investigation, the relevant staff recognised that the controls set out in s 220 may apply to the interview audio files and retrospectively sought advice from NZSIS Legal. After receiving that advice, NZSIS staff did not continue with the disciplinary investigation, and opted to implement a training plan for the Vetting Officer to prevent future inappropriate conduct.

Can the NZSIS access and use security clearance assessment information for disciplinary investigations?

76. I consider, as did my predecessor, that accessing vetting interview audio files for internal disciplinary purposes is not permitted under s 220. In this instance, while listening to the audio

[18] ISA, s 219.

files breached s 220, I consider that the NZSIS's decision to cease accessing the vetting files for the disciplinary investigation was appropriate.

77. The current NZSIS vetting quality assessment procedure limits quality assessments to checking Vetting staff's compliance with record-keeping requirements. This guidance is only for routine quality assessment purposes, however, and does not extend to disciplinary investigations. I note that NZSIS recently updated other policies and procedures relating to vetting information, including limiting information sharing and strengthening the language and guidance on s 220 restrictions. A similar amendment could be made to the quality assessment procedure, which would only apply to the Vetting Branch. Alternatively NZSIS could formalise a new procedure for all managers which would cover disciplinary investigations for all staff who have access to vetting information for their roles (eg Counter-Intelligence staff).

78. **Recommendation 3:** I recommend the NZSIS updates and promulgates guidance for managers on how section 220 limits use of security clearance assessment information for disciplinary investigations and the process for disciplinary investigations that involve or may involve such information.

79. I note that had the complaint against the vetting officer come to my office, under s 171 ISA, I could have accessed security clearance assessment information to investigate it. The ISA is clear that the Office of the Inspector-General is established to provide independent oversight of the agencies, including ensuring that any complaints about them are investigated independently.[19] Section 217 provides that for the purpose of performing its functions, the IGIS must be given access to all security records in the custody or control of the agencies. "Security records" is defined in s 4 as "papers, documents and records" that are officially made or received by an agency or an employee of an agency. I consider security records includes security clearance assessment information. In circumstances where NZSIS is bound by s 220, NZSIS may advise complainants that they can make a complaint to the IGIS.

COLLATERALLY OBTAINED INFORMATION

80. This review examined one further instance of a vetting officer sharing information obtained during a security clearance candidate interview with NZSIS counter-terrorism investigators.

81. In early 2019 a vetting officer emailed the Security Vetting Unit Manager (Vetting Manager) about a person discussed during a vetting interview. According to the security clearance candidate, this person had made social media posts of possible security interest.

82. Three days later the Vetting Manager forwarded the email to the NZSIS Counter-Terrorism group and the information was subsequently made available for a specific counter-terrorism investigation.

83. Shortly after the Vetting Manger was asked whether it was worth recording that the information provided was not vetting information. The Vetting Manager agreed it was.

[19] ISA, s 156.

84. On the face of it this appeared to be a straightforward instance of vetting information being disclosed within NZSIS for counter-terrorism investigation purposes, in breach of s 220. However, the Vetting Manager and the Vetting Officer's recollection was that the information was a 'tip off' from the candidate, not information supplied for the purpose of the candidate's security clearance assessment. The candidate wanted to give NZSIS information he thought would be of concern in the aftermath of the March 15 terror attacks. Despite the emails referring to the information being discussed at the interview, the Vetting Manager and Vetting Officer recollected that the candidate provided the information at the conclusion of the interview. In their view, the disclosure was not part of the vetting process, but separate to it. For that reason they thought it was not captured by s 220.

85. I think it possible a security clearance candidate could volunteer information before, during or after a vetting interview that is relevant to national security but not to their clearance. Most people rarely find themselves knowingly in conversation with an NZSIS officer. They cannot be expected always to limit the information they offer strictly to what is related to the vetting process. The NZSIS must be very careful, however, to record clearly and verifiably any instance in which a candidate discloses information separate from the vetting process. That did not happen in this case. I think also that Vetting should seek advice from NZSIS Legal before further sharing any such information.

86. The NZSIS advised my review that its current practice is to ask the candidate volunteering non-vetting information to submit it separately to NZSIS through the agency's "Virtual Walk-In" online portal. In my view that is a reasonable way to separate any such disclosure from the vetting process, providing a careful record is kept and a legal check obtained. The procedure should be set out in NZSIS vetting documentation, which should also make it clear that any such disclosures are exceptional, the information must be irrelevant to the security clearance assessment, and disclosures are not something vetting officers should actively solicit.

87. **Recommendation 4:** I recommend NZSIS revise vetting documentation to include:

- a procedure for handling disclosures of collateral non-vetting information by security clearance candidates, including directing the candidate to provide information separately by Virtual Walk-In;
- a requirement for Vetting staff to keep a full record of the information concerned and the basis for identifying it as separate from the security clearance process;
- a requirement for Vetting staff to seek confirmation from NZSIS Legal that the information is not subject to s 220; and
- guidance for vetting officers that they should not actively solicit disclosures of such information from candidates.

TRANSPARENCY TO SECURITY CLEARANCE CANDIDATES

88. As my predecessor commented, vetting records consist of some of the most confidential and sensitive information held by the New Zealand Government.[20] During the security clearance assessment, candidates may disclose, or the NZSIS may obtain, information about their mental health, drug and alcohol use, pornography, financial situation, and gambling activities.

89. At no point during the security clearance assessment process are candidates advised that the information provided to or obtained by the NZSIS may be accessed, used or disclosed for purposes outside of those listed in s 220. Candidates are not given the opportunity to either withdraw or refuse to answer any self-incriminatory questions. Before commencing the vetting application the on-line "Tiaki" vetting system informs candidates that the completed questionnaire is stored securely and that the information is not made available to other government agencies except to support the clearance recommendation.

90. The security clearance assessment process seeks absolute candour from the candidate with a reciprocal assurance of privacy from the NZSIS. In my view the assurances so far given from NZSIS overstate its compliance with the limitations imposed by s 220.

CONCLUSION AND RECOMMENDATIONS

91. I consider section 220 to be an absolute prohibition on use of security clearance assessment information outside of those listed in the Act. This review into NZSIS use and sharing of vetting found that the NZSIS has inconsistently interpreted and applied s 220. NZSIS has occasionally sought to use and disclose vetting in ways other than those allowed under s 220.

92. Section 220 protects the security of the security clearance system by restricting collateral use of this sensitive information. It is unlawful to use vetting information other than for counter-intelligence or security clearance assessments. Further, I do not consider an intelligence warrant can lawfully authorise access to and use of security clearance assessment information for other purposes. That is contrary to the authorisation framework of the ISA. A warrant cannot override a safeguard in the ISA itself.

93. I also do not think that s 220 prohibits *use* of security clearance information but permits *disclosure*. There is no meaningful distinction in practice that can be made between *use* and *disclosure* in the interpretation and application of s 220. Implying exceptions for certain information is clearly contrary to the purpose of the section. In fact, candidates are assured throughout the process that their information cannot be used for any other purpose.

94. The gaps in NZSIS policy and procedure provide for an operating environment where staff are not provided with fit for purpose guidance or information on s 220.

95. I make four recommendations.

---

[20] Above n 7 at [2].

- **Recommendation 1:** I recommend NZSIS cease applying for intelligence warrants to access security clearance assessment information contrary to s 220 ISA and revoke the Standard Operating Procedure on accessing vetting information under an intelligence warrant.

- **Recommendation 2:** I recommend NZSIS updates and promulgates the relevant internal policies and procedures including:

    - updates to the Policy regarding using vetting information for counter-intelligence activities and the Standard Operating Procedure on sharing vetting information within NZSIS, and

    - the development of a Standard Operating Procedure on sharing security clearance assessment information with other agencies.

- **Recommendation 3:** I recommend NZSIS updates and promulgates guidance for managers on how section 220 limits use of security clearance assessment information for disciplinary investigations and the process for disciplinary investigations that involve or may involve such information.

- **Recommendation 4:** I recommend NZSIS revise vetting documentation to include:

    - a procedure for handling disclosures of collateral non-vetting information by security clearance candidates, including directing the candidate to provide information separately by Virtual Walk-In,

    - a requirement for Vetting staff to keep a full record of the information concerned and the basis for identifying it as separate from the security clearance process,

    - a requirement for Vetting staff to seek confirmation from NZSIS Legal that the information is not subject to s 220, and

    - guidance for vetting officers that they should not actively solicit disclosures of such information from candidates.