Office of the Inspector-General of Intelligence and Security

Review of NZSIS framework for disclosing incidentally obtained information on crime to the Police

---

Public Report

Brendan Horsley
Inspector-General of Intelligence and Security
20 December 2021

CONTENTS

BACKGROUND

1. In late 2020 I reported publicly on my inquiry into a complaint that the New Zealand Security Intelligence Service (NZSIS or the Service) had failed to pass on information about serious crime, discovered during an intelligence operation many years ago, to the Police.[1] My inquiry found the Service had found information indicating that serious criminal offending was occurring and had not passed it on. I did not find, however, that the Service had acted improperly.

2. The Service had (and still has) discretion on whether to provide Police with information on crime discovered in the course of intelligence operations. In the case complained of, its decision appeared questionable, but there were no records of how it had been made. Some possible reasons against disclosure to the Police were at least conceivable. It was apparent, also, that the Service had not perceived the full scale and nature of the crimes of which the offender was later convicted.

3. At the time of the operation that prompted the complaint, the Service had no policy on disclosure of incidentally obtained information on crime to the Police. Following its own recent review of the incident, it quickly developed a standard operating procedure (SOP). I became aware of a relatively recent intelligence operation involving several decisions on disclosure to the Police. These decisions pre-dated the SOP, but were recorded in reasonable detail. I initiated the present review to examine those decisions and assess whether the SOP provided sound and useful guidance on how such decisions should be made.

THE ISSUE

4. This report concerns how the Service decides whether to disclose information on crime to the Police in very specific circumstances. The Service conducts intelligence operations – eg searches, surveillance, interception – to collect information relevant to national security. In doing so it can find information about criminal activity. Some such information will be relevant to the Service's intelligence purpose. For example, in monitoring a person suspected of violent extremism the Service might learn they have bought a weapon illegally. It would report that information, as intelligence, to relevant authorities, including the Police, because it is relevant to the national security threat the person presents. But the Service can also learn of criminal activity unrelated to its intelligence purpose. For example, in monitoring a person suspected of working covertly for a foreign government, it might learn that someone in their family has committed a serious assault. If the criminal activity has no connection to the activity the Service is investigating, it is not intelligence and the Service has no cause to report it as such. It is "incidentally obtained information": material the Service has come across while looking for something else. By law, the Service has discretion on whether it reports incidentally obtained information on crime to the Police. This review concerns how it makes that decision.

[1] Inspector-General of Intelligence and Security *Report into a complaint against the NZSIS* (30 November 2020).

SUMMARY OF FINDINGS AND RECOMMENDATIONS

5. This review has highlighted the difficulty of decisions about whether the Service should disclose incidentally obtained information about apparent serious criminal offending to the Police. In the case study reviewed, we found the Service generally approached these decisions in a considered manner and exercised its discretion appropriately. Review of current policy and procedure in light of the case study findings has identified possible improvements.

6. I recommend Service internal guidance on disclosure to Police of incidentally obtained information on crime is amended to specify internal consultation and information requirements more precisely; set out relevant considerations comprehensively in one place; add some particular requirements on how disclosures are to be carried out and recorded; and specify procedure for interim decisions not to disclose information. I recommend also that the Service work with the Police to:

   - revise their joint information sharing protocol to clarify the distinction between intelligence sharing and disclosure of incidentally obtained information; and
   - assess the potential for a process for exploring, by partial sharing of information, whether full disclosure of information on potential serious crime in any particular case would assist the Police or not.

LAW

7. One of the Service's core functions under the Intelligence and Security Act 2017 (ISA) is to collect and analyse intelligence in accordance with the Government's priorities and provide it to other people and organisations.[2] This includes the Police.[3] Whether and when the Service shares information with another agency as reportable intelligence is for the Service to decide.

8. In collecting intelligence, the Service may acquire information unrelated to its intelligence functions. The ISA refers to this as incidentally obtained information.[4] Section 104 of the Act allows the Service to disclose incidentally obtained information, at the Director-General's discretion, to organisations (including Police) in specified circumstances. The circumstance relevant here is where the Director-General "has reasonable grounds to believe" disclosure of information "may assist in … preventing or detecting serious crime in New Zealand or any other country". Serious crime is defined as any offence punishable by two or more years of imprisonment.[5]

9. Points to note on these provisions are:

   - The option of disclosure applies only to information relevant to the prevention or detection of *serious* crime. If the Service has incidentally obtained information on

[2] ISA, s 10.
[3] Intelligence sharing is authorised by the Minister responsible for the Service (ISA, s 10(1)(b)(iii)).
[4] Intelligence and Security Act 2017, s 47.
[5] ISA, s 47.

lower level offending with no apparent relevance to serious crime, disclosure to Police is not an option.

- The threshold of "reasonable grounds to believe" that disclosure "may assist" sets a reasonably permissive threshold for the Director-General to disclose incidentally obtained information. The requirement for reasonable grounds demands careful consideration and an explainable basis for belief. "May assist", however, allows disclosure when the Director-General decides that information is merely of possible value to the Police, rather than likely or certain value.

- The threshold of two years' imprisonment in the definition of serious crime is not high. It compares to a Category 3 offence under the Criminal Procedure Act 2011,[6] capturing offences such as aggravated assault, threatening to kill, dangerous driving and recidivist drink driving, usually tried in the District Court.

POLICY IN PLACE AT THE TIME OF THE CASE STUDY

NZSIS standard operating procedure

10. At the time of the case study examined for this review the Service had an SOP on the handling of inadvertent and incidentally obtained information. It set out the tests for disclosing incidentally obtained information under s 104 ISA and the statutory definitions of incidentally obtained information and serious crime. It required Service staff deciding whether to disclose information under s 104 to seek internal legal advice on the application of the thresholds in s 104; consult and obtain approval for disclosure from those responsible for collecting the information, to ensure collection methods were protected; and seek approval from the Director-General (or a delegate) for any disclosure.[7]

NZSIS-Police information sharing protocol

11. An information sharing protocol between the Service and the Police was endorsed in late 2018 by the two agencies. It is primarily concerned with routine intelligence sharing under s 10 ISA. It mentions the possibility of disclosure under s 104 ISA, but notes it will be relevant in limited circumstances.

12. The protocol lists principles to guide decisions about sharing information. Public safety and protection of New Zealand's national security are principal objectives. Other principles include maintaining operational effectiveness, collecting and sharing intelligence where necessary and proportionate, acting in accordance with law and human rights obligations, and protecting sources and methods.

13. It is not entirely clear, however, whether the principles set out in the protocol are intended to apply to disclosure of incidentally obtained information under s 104, as well as intelligence

---

[6] Criminal Procedure Act 2011, s 6.

[7] At the time, no delegations for decisions on disclosure under s 104 were in effect, so the Director-General was the only person who could approve disclosure.

sharing. The protocol is mainly concerned with intelligence and uses the words sharing and disclosure interchangeably.

14. The protocol notes that NZSIS information is generally shared for intelligence purposes only: the Service does not typically collect information as evidence and it will often not be available for use in criminal investigation or prosecution, even if it might have evidentiary value.

CASE STUDY

15. The case study examined for this review was a Service investigation involving close cooperation with the Police. While the individual was under investigation by NZSIS, there were four points at which the Service acquired information on potential criminal offending: three involving the target and one involving an associated person. For convenience I refer to these as incidents 1 to 4.

Incident one

Information	*NZSIS assessment*	*Outcome*
Criminal offence by target of NZSIS investigation.	Reportable intelligence.	Reported to Police as intelligence.

16. The Service learned that the target of its investigation had committed a criminal offence, apparently unrelated to the type of national security threat the Service was concerned with. It considered whether to report this to the Police as intelligence (under s 10 ISA) or disclose it as incidentally obtained information (under s 104). Records indicate it initially considered disclosure, then decided to reframe the information as intelligence.

17. The Service is entitled to rethink an initial assessment and in this instance I consider it was open to the Service to provide the information to Police as intelligence. A link between the crime and the national security threat presented by the target was not immediately evident, but an argument that it was relevant could be made.

18. Ultimately, however, it was not very clear why the Service proceeded to provide the information in an intelligence report. After acquiring the information the Service soon learned that the Police already knew of it, were investigating and considering prosecution. By the time the Service reported its information to Police, the Police already knew the key points, to the Service's certain knowledge. The Service did not provide any analysis of the significance of the information for national security, beyond saying its significance was unclear.

19. The end result was arguably an intelligence report to the extent that it provided information on a target of mutual interest with some source material the Police probably did not already have. It is for the Service to decide what constitutes worthwhile intelligence reporting, but in this instance I concluded that a more methodical evaluation of its purposes in sharing the information would have clarified how it was fulfilling its intelligence function.

Incident two

Information	*NZSIS assessment*	*Outcome*
Criminal offence by person associated with target of NZSIS investigation.	Incidentally obtained information.	Disclosed verbally to Police, but written disclosure deliberately avoided.

20. This incident concerned information acquired by the Service about criminal offending by a person associated with the target of its investigation. The Service verbally disclosed this to Police, under s 104 ISA, as incidentally obtained information. A few weeks later it decided against 'formally' disclosing the information in writing, out of concern for the impact any Police action might have on the target's behaviour and any consequential prejudice to the Service's operation. It decided to retain the information for 60 days, for possible later disclosure. If not disclosed within that period the source material would be destroyed.[8] The Service did not revisit its decision against written disclosure and apparently destroyed the information.

21. The Service's assessment of whether the relevant offending met the serious crime threshold, its analysis of the basis for disclosure under s 104 and its consideration of whether disclosure might assist the Police to detect offending were robust. Its consideration of the possible effect of disclosure on its investigation was appropriate: that is the balancing of law enforcement and national security concerns the legislation is designed to enable.

22. In my view it was also open to the Service to delay disclosure to manage any risk to its operations. I do not think 60 days an unreasonable period to hold information that might be relevant to law enforcement, pending possible disclosure.

23. The Service does however seem to have assumed disclosure to Police would necessarily have resulted in disruption to its operation. It made no attempt to work with Police to identify how the anticipated risk could be mitigated.

24. The Service also made an invalid distinction between verbal and written disclosure. Once it had verbally briefed the Police it had disclosed the information. The disclosure was lawful, as the Service had reasonable grounds to believe it would assist the Police in preventing or detecting serious crime. Unfortunately the Service then decided against 'formal' disclosure in writing. That was simply artificial.

Incident three

Information	*NZSIS assessment*	*Outcome*
Criminal offence (different to that in incident 1) by target of NZSIS investigation.	Reportable intelligence.	Not reported or disclosed to Police.

[8] In accordance with s 104, which provides that the Service can only retain incidentally obtained information only for the purpose of disclosure.

25. Incident three concerned offending by the target, of a different type to that in incident one. This behaviour had been noted in past Service intelligence reporting supplied to the Police. The Service knew from its intelligence collection that the offending was continuing, some months later. It considered whether it should report this as intelligence or disclose it as incidentally obtained information; decided it was reportable intelligence and began drafting a report; then finally decided against reporting.

26. In my view it was open to the Service to assess the information as reportable intelligence rather than incidentally obtained information on crime. A link could be made, albeit not a particularly strong one, between the criminal activity and the national security risk presented by the target. The Service's analysis set out the connection.

27. Ultimately the Service's decision not to report the information to Police was bound up with and subsumed by its decision against disclosing the information arising in incident two, about the offending by the person associated with the target. It was nonetheless a decision the Service was entitled to make, given its normal discretion on when and what to report as intelligence.

28. I note, however, that having assessed the information about the target as reportable intelligence, the Service should have separated it from the proposed disclosure about the target's associate. That would have ensured a clearer record of the decisions reached on each matter.

Incident four

Information	*Assessment by NZSIS*	*Outcome*
Behaviour by target related to the offending in incident 3, but possibly indicating more serious criminal intent.	Not identified by NZSIS as distinct from the offending in incident 3.	Not reported or disclosed to Police.

29. Incident four involved behaviour by the target related to the offending observed by the Service in incident three, but possibly indicating a more serious development of it.

30. From the records reviewed, the Service did not see this behaviour as raising any new issue. It did not therefore consider whether it was reportable intelligence or incidentally obtained information it might disclose to Police.

31. Had the Service done so, it might have linked the information again to the national security risk presented by the target, and considered it reportable intelligence. It is also possible, however, to see how it might have been considered more directly relevant to the prevention or detection of serious crime. As it happened the Service neither reported nor disclosed the information. It was a point of detail in a stream of information the Service was assessing for intelligence on a national security threat. It was recorded without prompting any special scrutiny.

32. I do not fault the Service for not focussing its attention and analysis on a particular item of information potentially relevant to criminal activity of a type that was not its prime concern. While not inattentive to the target's criminal behaviour, the Service was more closely focused on other risks.

33. Nonetheless, had Service lawyers been supplied with the relevant source material when answering other questions on disclosure in this case (which could easily have occurred), the behaviour concerned might have been noted and its relevance to the prevention of crime considered. It is not difficult to envisage other situations in which a lawyer might have a different appreciation of raw intelligence relating to crime than an intelligence analyst.

34. I think this incident indicates the importance of ensuring that decisions on whether to disclose incidentally obtained information potentially relating to serious crime are informed by all relevant information. Investigators would also benefit from better guidance on categories of crime-related information they should be alert for.

POLICY DEVELOPED SINCE THE CASE STUDY

35. As noted in the introduction to this report, after the events of the case study (but not because of them) the Service developed an SOP for disclosure of incidentally obtained information on serious crime.

36. The SOP details the circumstances in which incidentally obtained information on serious crime can be disclosed, with reference to s 104 ISA and the Act's definition of serious crime. It states a procedure for determining whether the information relates to serious crime and whether it is reportable intelligence or incidentally obtained information that should be disclosed under s 104. It specifies who can authorise disclosure, some record keeping requirements and how disclosures are to be drafted and classified.

37. The SOP also refers staff to a guidance note on disclosure of incidentally obtained information. The guidance note is training material, with similar content to the SOP but more detail on factors to consider when deciding whether to disclose incidentally obtained information. The guidance note also lists possible risks to Service operations or information from disclosure of incidentally obtained information to the Police.

ANALYSIS OF THE CURRENT FRAMEWORK

Exercise of discretion on disclosures to the Police

38. The Service has discretion on whether or not to disclose incidentally obtained information on crime to the Police. If considering disclosure it must under s 104 have reasonable grounds to believe that it may assist in preventing or detecting serious crime. Having the requisite belief does not however oblige the Service to disclose. It has room to exercise judgement.

39. There is good reason for this discretion. The Service is charged with protecting national security, an important public purpose. Law enforcement is also an important public purpose, but crime varies widely in the immediacy, severity and scope of its impacts. An obligation on the Service

to disclose any and all incidentally obtained information on crime to Police could disrupt intelligence operations, causing harm that exceeds any benefit to law enforcement. Disclosure to Police might, for example, lead to Police action that alerts a Service target that they are under investigation, prompting them to "go dark" and/or accelerate plans to commit harm. The ISA acknowledges this risk both by limiting the scope for disclosure to information relevant to the prevention or detection of serious crime and by allowing the Service discretion even where the crime is serious.

40. Further, Police powers to investigate crime are subject to constraints that protect fundamental rights and liberties, such as the constraints on searches under the Search and Surveillance Act 2012. The Service has more intrusive powers, given the importance attached to countering threats to national security. The threshold for the Service to obtain a warrant to search, for example, is lower than it is for the Police. This is counterbalanced by its lack of any enforcement function. Enabling or obliging the Service to disclose to Police any and all information on crime – or even serious crime - incidentally obtained through intelligence operations would result in the Police being more frequently supplied with information they could not lawfully acquire using their own powers. Discretion for the Service means this occurs only exceptionally, subject to case-by-case assessment of the relative importance of the intelligence and law enforcement interests at stake.

41. The ISA does not state what the NZSIS Director-General should consider when exercising that discretion. The Service guidance note (see above paragraph 37) lists some relevant factors, but they are focused almost entirely on the Service's operational interests. In addition, I think the following considerations apply to decisions on disclosing incidentally obtained information on crime:

- The nature and gravity of the crime at issue. While the threshold in s 104 is that the information held by the Service may assist in preventing or detecting serious crime, the statutory definition of serious crime encompasses a broad range of offences (see paragraph 9 above). Assessing the gravity of relevant offending would mean considering additional matters such as the nature of the possible harm (eg to people or property); whether it is historic or current; whether it is imminent, ongoing, or a single incident; and the number and vulnerability of any actual or anticipated victims. In addition to recognising the relevance of these factors, Service policy could identify categories of serious crime information that should prompt careful consideration and escalation of decision-making, eg information on crime involving imminent or recent physical harm to a person; relating to organised crime; or relating to particularly vulnerable persons (such as children).

- Where any factors weigh against disclosure to the Police, the Service should consider what steps could be taken to reduce their impact, eg obscuring the Service's sources or timing disclosure to avoid or minimise disruption to its operations.

42. A difficult question for the Service is the extent to which the Police might be able (or unable) to make effective use of the information. Section 104 requires the Service to have reasonable grounds to believe that disclosure "may assist" in preventing or detecting serious crime, but there are limitations on the ability of the Service to assess what the Police can or cannot do with information supplied. Although the Service might at any given time have staff who have experience of working with the Police, or in the Police, or in criminal law, criminal investigation is not the Service's core business. The Service also does not necessarily know whether the Police already have the information concerned, or whether disclosure will make any significant difference to what the Police already know. It does not necessarily know what priority the Police will give to any further investigation. As a general rule, when disclosing information to the Police, the Service prefers it not to be used as evidence in criminal proceedings, and so any disclosure can be subject to caveats designed to prevent that. These will clearly limit the utility of the information to Police. All these factors can produce significant uncertainty over whether disclosure "may assist".

43. In my view there will at least sometimes be scope for the Service to explore with Police whether a certain disclosure might assist them. This would need to be done without full disclosure of the information concerned, but in some circumstances this should be possible. The Service might, for example, explain in general terms the kind of information it has come across, which criminal offences seem relevant, any constraints it anticipates on what it could disclose, and any questions it has about the utility of the information to Police, without disclosing details such as the names and location of people involved. With partial information the Police might only supply tentative advice, but that could still assist the Service in making a decision.

Recommendations

44. Overall, this review did not identify fundamental flaws with Service's framework for decisions on disclosure of incidentally obtained information on crime to the Police. It has however identified specific areas for improvement.

Statutory basis for providing information

45. This review has highlighted the importance of the initial assessment, once serious crime information has been identified, of whether it is reportable intelligence or incidentally obtained information that may be disclosed under s 104. That is not always an easy question to answer. It requires both intelligence and legal expertise. The examples reviewed showed the valuable contribution legal advice can make, but existing Service guidance does not require consultation with the Service legal team on the basis for providing information (ie reporting under s 10 or disclosing under s 104). I think it should. It should also stress the importance of decisions being fully informed by all relevant material.

Recommendation 1

I recommend Service guidance is amended to:

- Require operational staff to consult the legal team on decisions about whether collected information about crime is reportable intelligence or incidentally obtained information; and

- ensure all those advising and deciding on disclosure have a full and accurate account of the serious crime information at issue, including relevant primary source material.

46. This review found it was not entirely clear whether the principles set out in NZSIS-Police information sharing protocol applied to disclosure of incidentally obtained information under s 104 as well as intelligence sharing. This uncertainty is not ideal, as the protocol is an important reference for both parties.

Recommendation 2

I recommend the Service work with Police to revise their information sharing protocol to clarify the distinction between intelligence sharing under s 10 ISA and disclosure of incidentally obtained information on crime under s 104, and the principles applying to each.

Exercise of discretion to provide information

47. Service guidance for staff on the exercise of discretion under s 104 is contained in both its SOP and a guidance note. This review found also that although the factors listed in the guidance note are relevant, they are focussed on the Service's operational interests and other factors deserve consideration.

Recommendation 3

I recommend the Service amend its guidance on potential disclosure of information on serious crime to set out relevant considerations comprehensively in a single document, including:

- factors in the gravity of offending that meets the statutory definition of serious crime, including any that will weigh heavily in favour of disclosure and any that will allow greater discretion against disclosure; and

- how the Service will assess risks to its operations that might arise from disclosure and what mitigations it will consider for the purpose of enabling disclosure while protecting sources and methods.

48. In addition to setting out relevant factors, the Service could take the further step of specifying categories of serious crime information that should be promptly referred to management and the legal team for consideration. I have suggested, for example, information on crime involving imminent or recent physical harm to a person; relating to organised crime; relating to particularly vulnerable persons (eg children).

Recommendation 4

I recommend the Service consider amending its guidance to specify categories of serious crime information that should be promptly referred to management and the legal team to determine whether disclosure to Police under s 104 is required.

Engagement with Police on potential value of disclosure

49. This review has noted that it can be difficult for the Service to assess whether disclosure of indentally obtained information to Police under s 104 "may assist" in the prevention or

detection of serious crime, but there may be unexplored scope to test this with Police, in particular cases, by sharing information short of full disclosure.

Recommendation 5

I recommend the Service work with Police to assess the potential for a process for exploring, by partial sharing of information, whether full disclosure of information on potential serious crime would assist the Police or not.

Verbal vs written disclosure

50. In incident two, the Service verbally briefed the Police on information it anticipated disclosing under s 104, but eventually decided against disclosure in writing. That was an artificial distinction: s 104 does not limit the meaning of disclosure to written communication and on a natural reading it must include verbal communication. Disclosure in writing is good practice for record keeping purposes and is the current position in the NZSIS-Police information sharing protocol.

Recommendation 6

I recommend the Service amend its guidance to clarify that disclosure under s 104 may be either verbal or written; that writing is preferable; and that a written record must be made of any verbal disclosure.

Formally distinguishing disclosure from intelligence reporting

51. In incident three the Service included reportable intelligence in a draft briefing note for a disclosure under s 104. A disclosure to the Police under s 104 is an exceptional departure from normal NZSIS intelligence reporting. To ensure a clear record of decisions on what to report and disclose, and avoid any possible confusion about the basis on which information is being provided I think a strict formal distinction should apply.

Recommendation 7

I recommend that Service guidance require reportable intelligence and disclosures under s 104 to be provided in separate and distinct formats to recipients.

Decisions to postpone disclosure

52. In incident two the Service decided against immediate disclosure of information to Police but reserved the option of disclosing later. This is an available and appropriate choice for the Service in some circumstances, but existing procedure does not acknowledge the possibility and provides no guidance on it.

Recommendation 8

I recommend the Service's policy guidance is amended to cover interim decisions not to disclose information, requiring that if a possible disclosure is postponed, the reasons are recorded; a timeframe is set for revisiting the decision; and when a final decision is made, reasons for that decision are recorded.

Record keeping

53. This review, like others, found that some information necessary to understand Service decision-making was stored in staff email inboxes rather than the system of record. The Service acknowledges that its record keeping practice regarding email requires improvement.

Recommendation 9

I recommend the Service remind its staff of the need to save all email relevant to investigations and decision-making to the system of record.