Te Pourewa Mātaki
Inspector-General of Intelligence and Security

Inquiry into GCSB's hosting of a foreign capability

Brendan Horsley

Inspector-General of Intelligence

March 2024

CONTENTS

SUMMARY

1. I have conducted an inquiry into the Government Communications Security Bureau's (GCSB's) hosting of a signals intelligence system deployed by a foreign agency and also taking part in a wider intelligence programme related to this capability ("the capability"). I was alerted to the existence of the capability by the GCSB, after it was discovered in an internal audit and questions were raised about its authorisation and how it operated.

2. I was concerned that the Bureau had apparently decided to host in New Zealand a signals intelligence system controlled by a foreign partner agency without seeking ministerial approval and without subsequently informing its minister of the system's existence or purpose. I was concerned also that the Bureau's current senior leadership and legal team apparently knew nothing of the system until it was brought to their attention in 2020.

How the capability functioned?

3. The details of the capability are highly classified, limiting the detail I can provide in a public report. Broadly, the capability produced intelligence that could help find remote targets.

4. There were many reasons why the capability might be tasked, but a key question for my inquiry was whether the capability could be used to support military operations. Based on the information reviewed, I found that the capability clearly had the potential to be used, in conjunction with other intelligence sources, to support military action against targets. The circumstances of the tasking would determine whether material support had been provided or not. The sensitivity of this issue was clearly identified by the GCSB when it was considering hosting the capability back in 2010.

How the Bureau decided to host the capability

5. I found, in relation to the Bureau's decision to host the capability:

    5.1. The GCSB undertook a reasonably robust investigation into the capability and the potential issues with hosting it. This included consulting the relevant international partners, which resulted in potential concerns being raised by GCSB staff about the operation of the capability in New Zealand.

    5.2. When considering hosting the capability, the GCSB identified legal and policy concerns, including the potential for the capability to be used to support military operations. These concerns were circulated at the most senior level of the GCSB.

    5.3. The record-keeping of the decision process was poor and there are significant gaps, which have made it difficult to identify reasons for certain decisions, particularly whether concerns about the capability were mitigated by redrafts to the MOU. There appears to be no substantive written legal advice, despite the GCSB's General Counsel being involved throughout the process.

5.4. Despite the then acting Director-General anticipating that the Minister responsible for the GCSB would be informed about the capability and possibly asked to approve GCSB hosting the system, this inquiry found no evidence of the Minister being told about the capability

5.5. The decision to host the capability on the terms set out in the MOU was significant, particularly given the potential uses of the capability to support military operations. It was a matter the Minister might have considered putting to Cabinet or selected Ministers. The Bureau should have briefed the Minister in accordance with the "no surprises" principle.

5.6. Though the authorisation process for intelligence sharing at the time seems manifestly inadequate, a Ministerial authorisation in place in 2012 for the GCSB to share intelligence and cooperate with the foreign partner was broad enough to cover the capability and so the decision to host the system without further Ministerial approval was lawful.

5.7. It was improper, however, for the GCSB to decide on hosting the capability without bringing it to the Minister's attention. By doing so it failed to respect and enable Ministerial control of the agency.

5.8. It would have been prudent for the GCSB to notify the Inspector-General of Intelligence and Security at the time of the decision to host the capability.

How the capability operated at GCSB

6. Due to issues with record-keeping and the passage of time, it was difficult to obtain clear information about how the capability operated. My inquiry was able to find at least 45 instances of the capability being tasked over the period of operation, but I also found information to suggest that this does not represent the full history of tasking. Some tasking was apparently able to occur without GCSB knowledge.

7. I found that the capability operated at GCSB:

7.1. without adequate record keeping;

7.2. without due diligence by GCSB on the capability tasking requests;

7.3. without full visibility for GCSB of the capability tasking;

7.4. without adequate training, support or guidance for GCSB operational staff;

7.5. with negligible awareness of the capability at a senior level within GCSB after the signing of the MOU in 2012 and until the system was shut down in 2020;

7.6. with no apparent access for GCSB to the outcomes of the capability's operation at GCSB;

7.7. without any auditing;

7.8. without the required review of the MOU;

7.9. without due attention to the possibility, recognised within the Bureau, that support for the capability could contribute to military targeting; and

7.10. without clarity, in consequence, as to whether data supplied by the GCSB to the capability did in fact support military action.

8. I note that the risk of GCSB support for the capability contributing to military action was moderated significantly by the geographical limits of GCSB collection. However, I find that the way in which the capability was operated meant that the Bureau could not be sure the tasking of the capability was always in accordance with Government intelligence requirements, New Zealand law and the provisions of the MOU.

Conclusion and recommendations

9. As the hosting of the capability has now ceased, a key question for my review was whether there was a risk of the shortcomings I identified being repeated.

10. The GCSB's operations, governing statute, policies and compliance systems have changed significantly over the period in which the capability operated. Oversight from my office has also developed significantly. The GCSB also has a Joint Policy Statement on International Agreements and Arrangements which provides a robust framework for when the GCSB enters into arrangements such as the MOU for the capability. These developments have reduced the risks of the issues I have identified in the GCSB's hosting the capability reoccurring.

11. Alongside these organisational developments, I also recommended that the GCSB undertake some actions to further mitigate the risk of these issues arising again. I recommended that the GCSB:

11.1. produce internal guidance to reflect existing requirements that international agreements and arrangements of significance are consulted with the Minister;

11.2. compile a register of collection or analysis capabilities in New Zealand that are operated by foreign partners;

11.3. undertake an audit of its systems, including any foreign partner capabilities. I note that this is already underway;

11.4. initiate a programme of work to review and monitor international agreements and arrangements within specified timeframes; and

11.5. establish processes which enable my office to view new international agreements and arrangements when entered into.

12. The GCSB has accepted all recommendations.

BACKGROUND

13. In 2012 the Government Communications Security Bureau (GCSB or the Bureau) agreed to host a signals intelligence system deployed by a foreign agency ("the capability") and take part in a wider intelligence programme related to this capability. The capability involved:

    13.1. GCSB hosting partner-supplied and controlled hardware in a GCSB facility;

    13.2. the capability selecting and transmitting certain signals, collected by GCSB under authorisation, to the partner agency through the hardware; and

    13.3. the transmitted signals being analysed, in combination with other information, to produce intelligence that could help find remote targets.

14. The capability operated from 2013 until 2020, when it was stopped by an equipment failure.

15. After its installation, senior GCSB staff and the Bureau's legal team lost sight of the capability and its operation. It was "rediscovered" at a senior level following concerns being raised in 2020 about another partner system hosted by GCSB.

16. In late 2020, the Bureau alerted me to the existence of the capability and highlighted potential concerns about whether it had been operating unauthorised. The GCSB advised me that it was investigating the matter. GCSB leadership also directed that the system not resume operating.

17. From its investigation the GCSB found that the capability had been installed under a Memorandum of Understanding (MOU) agreed between the Bureau and the foreign partner agency. There was no indication, however, that the Minister responsible for the GCSB had been briefed on the system, or asked to approve it. The MOU had a clause requiring it to be reviewed within 24 months and every three years thereafter, but this had not been done.

18. The Bureau concluded, however, that at the time of its report the operation of the capability was authorised by an intelligence warrant issued in 2020. The application for the warrant had not mentioned the capability, because those responsible for the application were not aware of it, but the Bureau considered that its operation nevertheless fell within the scope of the warrant.

19. I was concerned that the Bureau had apparently decided to host in New Zealand a signals intelligence system controlled by a foreign partner agency without seeking ministerial approval and without subsequently informing its minister of the system's existence or purpose. I was concerned also that the Bureau's current senior leadership and legal team apparently knew nothing of the system until it was brought to their attention in 2020. I decided to inquire into:

    19.1. what the capability was;

19.2. how the GCSB decided to host the capability;

19.3. how the capability functioned at GCSB; and

19.4. whether the operation of the capability was authorised.

20. The capability did not resume operation after the equipment failure in 2020. The Bureau subsequently decided to terminate its support for the system and returned the hardware to the partner agency.

Inquiry process

21. My inquiry involved reviewing a large number of historic records from the GCSB system and seeking information and explanations from GCSB officials. I have also talked to GCSB staff with knowledge of the capability, although most of the staff who had close knowledge of the system in the most relevant years are no longer with the GCSB. I provided my draft reports to key former staff, included the relevant former Directors-General of the GCSB.

22. I was not able to access systems or discuss the operation of the capability with the foreign partner agency responsible for it. This limited my ability to determine fully how the capability operated, as the system at GCSB was only a component of a wider programme. It became apparent that the GCSB had little knowledge of the operation of the wider programme and the planning of the system being tasked. I have found some of the GCSB's explanations about how the capability operated and was tasked to be incongruous with information in GCSB records from the time.

WHAT IS THE CAPABILITY?

23. The details of the capability are highly classified, limiting the detail I can provide in a public report. My classified report details the nature and purpose of the system, the coordination of its use, how the capability was tasked, how the results of the capability were stored, and the key uses of the capability.

24. Broadly, the capability produced intelligence that could help find remote targets.

25. There were many reasons why the capability might be tasked, but a key question for my inquiry was whether the capability could be used to support military operations. Based on the information reviewed, I found that the capability clearly had the potential to be used, in conjunction with other intelligence sources, to support military action against targets. The circumstances of the tasking would determine whether material support had been provided or not. The sensitivity of this issue was clearly identified by the GCSB when it was considering hosting the capability.

HOW DECISIONS WERE MADE BY THE BUREAU ON THE HOSTING OF THE CAPABILITY

26. While I am unable to provide full details in this report on the process followed by the GCSB to host the capability, the following is a summary of key events.

27. The GCSB was identified in 2009 as a potential site to host the capability.

28. Senior officials at the GCSB discussed possible issues with hosting the capability, including its potential to support military operations. The then Director-General, Sir Bruce Ferguson, reportedly had "no problem" with GCSB prospectively hosting the capability. Other senior officials thought hosting it was an "operational call".

29. Following these discussions, a senior staff member at the GCSB noted "some potential legal and policy issues" and recommended that officials meet to discuss further. No minutes of this meeting could be found. A Powerpoint presentation prepared for the meeting detailed what the GCSB understood about the capability at the time, including its potential military applications. The presentation raised questions for the meeting about the legal and moral issues that might arise from hosting the system. It identified a need for a procedure for the GCSB to vet the tasking of the capability.

30. GCSB staff then engaged with overseas partner agencies to get further information about the capability. This included engaging with the partner agency that ran it and another partner agency that hosted it. Discussion included common concerns about the potential use of the capability for supporting military action. GCSB staff also noted there might be "oversight concerns". A report of these discussions was shared within the GCSB.

31. In late 2010 a senior GCSB officer signed an agreement in principle to host the capability. The letter noted the purposes of the capability, which included the potential use for military action. It recognised the value of the GCSB being involved. It highlighted that some operational scenarios would need careful handling to ensure compliance with New Zealand law, but the issues were not unmanageable.

Memorandum of understanding to host capability

32. In 2011 the GCSB worked on an MOU to host the capability. The process involved further debate about the potential for the capability to support military action against targets and the need for the GCSB to have control over its tasking. This was raised at the most senior level within the GCSB. A series of meetings was held to discuss the matter, but no notes or records were made.

33. Late in 2011, the then Director-General, Simon Murdoch, noted in an email that GCSB legal would need to be closely involved in the matter and that it would potentially require the awareness or consent of the Minister, as well as consultation with the IGIS. This inquiry found no record that the legal analysis, consultation and engagement with the Minister or IGIS contemplated by Mr Murdoch occurred.

34. There was substantial engagement between key GCSB staff about the terms of the MOU. Ultimately the staff member who had raised concerns about possible use for military purposes advised others that the draft MOU addressed those concerns.

35. Simon Murdoch's tenure as Acting Director-General ended the week before Christmas 2011. On 3 February 2012 Ian Fletcher took over as Director-General.

36. The MOU was signed in March 2012 by a GCSB Deputy Director. My inquiry found no records to indicate the Director-General was involved. Mr Fletcher advised the inquiry that he did not recall being briefed on the capability when he started at the GCSB, and has no recollection of the capability operating at GCSB or of Simon Murdoch's concerns.

Analysis of decision-making process

37. It is clear from records that from the outset the GCSB recognised legal and policy issues with hosting the capability, particularly its potential use for supporting military action. GCSB staff had in-depth knowledge of this and how the capability's predecessor had been used. They investigated the system through engagement with overseas partners. Senior officials at the GCSB, including two Directors-General, were informed about the nature of the system and the issues arising.

38. Legal staff were also involved relatively early in the process and continued to be involved up to the signing of the MOU, including in its drafting. There appears, however, to have been a lack of substantive written legal advice, which might have demonstrated whether and how legal concerns about the capability were addressed.

39. It is not clear from the records how concerns about the capability's potential use for military purposes were mitigated, other than the email that the wording of the MOU had addressed concerns (paragraph 34 above). The records show that in the nearly two years leading up to signing the MOU the Bureau understood the capability as directly associated with military applications. There are, however, no records of any substantive analysis to show how concerns raised about this were dealt with. An offer to remove the capability for such targeting was not taken up, but it is not clear whether it was given serious consideration.

40. Acting Director-General Murdoch's email in late 2011 (paragraph 33 above) shows clearly that he did not think a final decision on hosting the capability had been made at that point. He anticipated further analysis of legal risk and presumed the Bureau would brief the Minister and possibly the IGIS. This inquiry found no records of any further analysis or consideration of these matters between late August 2011 and the signing of the MOU by a Deputy Director at GCSB in March 2012.

41. The MOU included provisions for GCSB to ensure tasking of the capability was compliant with New Zealand law and Government expectations regarding foreign partner agency activities in New Zealand. This might have been considered sufficient mitigation of any risks or concerns, but this inquiry found no records of any such analysis.

Was the Minister told?

42. It seems clear the decision to sign the MOU and host the capability was not put to the Minister responsible for the GCSB, or any other Minister. This inquiry found no record of any Ministerial briefing or decision, nor any reference to any having occurred. It found no record of the Minister having been informed of the matter at all.

43. This apparent lack of reference to the Minister occurred despite the view expressed by Mr Murdoch that the Minister would likely need to at least be aware of, or consent to, the hosting of the capability.

44. None of the former staff I consulted as part of the inquiry recalled the capability, with many noting the time that has passed since their involvement.

Should the Minister have been briefed?

45. Cabinet Manual guidance in effect at the time on the relationship between Ministers and officials included, as its first point, that:[1]

> In their relationship with Ministers, officials should be guided by a "no surprises" principle. As a general rule, they should inform Ministers promptly of matters of significance within their portfolio responsibilities, particularly where these matters may be controversial or may become the subject of public debate.

46. The key factor in when a Minister should be briefed, as since affirmed in guidance from the Solicitor-General[2] and by the Courts[3], is the significance of the matter within the portfolio.

47. I think it straightforward that the GCSB should have briefed its Minister on its proposed hosting of the capability, in accordance with the 'no surprises' principle, considering that:

47.1. the GCSB staff apprised of the matter unquestionably saw the decision to host the capability as significant, given the extensive information they compiled and discussed about the history of the capability and the nature of the issues they raised;

47.2. the acting Director-General became engaged with the decision-making process, noted that the chief legal adviser would need to be "closely involved" and presumed the Minister would have to "at least" be made aware;

47.3. the GCSB was proposing to agree to a formal MOU with another state to host a system, largely controlled by the partner agency, for which the GCSB would be providing intercepted signals; and

47.4. the information the GCSB had to hand was that a prime use of the capability's data had been to support military action, particularly when tasked "ad hoc".

---

1 Cabinet Manual 2008 at 3.22. The guidance in the current Manual is substantially the same, omitting "As a general rule".
2 Solicitor-General "Chief Executives and the 'no surprises' principle" (6 September 2016, updated 2020) at [11].
3 *Peters v Bennett* [2020] NZHC 761 at [206].

48. The Cabinet Manual also provides guidance on what a Minister should put to Cabinet:[4]

> 5.11 As a general rule, Ministers should put before their colleagues the sorts of issues on which they themselves would wish to be consulted. Ministers should keep their colleagues informed about matters of public interest, importance, or controversy. Where there is uncertainty about the type of consideration needed, Ministers should seek advice from the Prime Minister or the Secretary of the Cabinet. Similarly, departments should seek advice from the office of the portfolio Minister, or from the Cabinet Office.
>
> 5.12 The following matters must be submitted to Cabinet (through the appropriate committee):
>
> a. significant policy issues;
>
> b. controversial matters;
>
> c. proposals that affect the government's financial position, or important financial commitments; […]
>
> m. international treaties and agreements[5]

49. Had the GCSB should informed its Minister, the Minister could have then decided whether to brief Cabinet colleagues. As it happened the Minister was not given the opportunity to consider this.

Was the Minister's approval required?

50. The proposed hosting of the capability would result in GCSB-collected data being provided to the foreign partner. Whether this required Ministerial approval hinged on the statutory regime for intelligence sharing in effect at the time. In short my analysis (set out in the Appendix) is that the legislation empowered the GCSB to collaborate operationally with partner agencies, and to share intelligence subject to Ministerial authorisation.

51. Authorisations for intelligence sharing were sought, at the time, without any supporting information. The Minister was simply presented with an authorisation to sign. There was nothing further by way of an application. The authorisations themselves simply stated that sharing intelligence with a state list of foreign agencies was permitted.

52. A Ministerial authorisation dated 2008 and apparently still in effect when the capability was being hosted stated:

> Under section 8(1)(d) of the Government Communications Security Bureau Act 2003 ("the Act"), I hereby authorise the Director of the Government Communications Security Bureau ("the Bureau"), or any person appointed as Acting Director of the Bureau in accordance with the provisions of section 10 of the Act, to provide reports on foreign intelligence to the Minister responsible for the Bureau and any or all of the persons or

---

4 At 5.11.

5 The agreement to host the capability does not appear to classify as an international agreement, as this is concerned with international treaties or the like (Cabinet Manual at 5.73 and 5.74). I note that there has been a change in practice by the intelligence agencies to refer to an agreement such as this as a "Memorandum of Arrangement" due to concerns that some Treaties can be MOUs. This change in practice is reflected in the JPS on International Agreements and Arrangements.

> office holders, whether in New Zealand or abroad, identified in the Schedule to this authorisation.

53. The schedule to the authorisation listed a large number of agencies in New Zealand and other countries, including the foreign partner in question. The authorisation had no further provisions regarding the scope of sharing authorised or how it was to be conducted.

54. When hosting the capability was proposed, therefore, the GCSB was authorised to share reports on foreign intelligence (which I have concluded must be read to encompass data likely to contain or produce intelligence) with the foreign partner.

55. The capability was, however, unknown to the Minister when the authorisation was signed. Hosting it was a significant development in the intelligence sharing arrangements between the GCSB and the foreign partner. I have already set out why I think it was significant enough to require briefing the Minister on a 'no surprises' basis (paragraph 47 above). In addition I see it as a significant development in intelligence sharing with the foreign partner considering that:

55.1. it would involve installing hardware at GCSB premises that could be operated remotely by the foreign partner;

55.2. the initiative in any transfer of GCSB data through the capability would lie with the foreign partner, not GCSB, unless a change was required; and

55.3. GCSB would concur by default with the tasking of the capability.

56. The importance of these factors is underscored by the preamble of the MOU (discussed further below):[6]

> New Zealand will only allow foreign governments to operate in, through or from its territory or assets with the full knowledge and concurrence of the New Zealand Government. All facilities, assets and systems used by a foreign government […] will operate in a manner which provides the New Zealand Government with full knowledge and concurrence of activities undertaken in, through or from New Zealand territory or assets.

57. Significant though it was, it is difficult to argue that hosting the capability took the intelligence sharing relationship with the foreign partner beyond the scope of the existing Ministerial authorisation. That authorisation was broad and unqualified.

58. The legislation at the time stated no factors the Minister was required to consider when authorising intelligence sharing. That does not mean the Minister had unfettered discretion: there is no such thing.[7] The authorisation was subject to the objects of the GCSB Act and the general law (including the Bill of Rights Act 1990). From that I think it inarguably

---

6 MOU paragraphs III/A and B.

7 *Air New Zealand v Wellington International Airport Ltd* [2009] NZCA 259, [2009] 3 NZLR 713 at [148]; *Unison Networks Ltd v Commerce Commission* [2007] NZSC 74, [2008] 1 NZLR 42 at [53].

followed that relevant considerations included, for example, all human rights obligations recognised by New Zealand law.

59. I cannot see, however, how the authorisation process supported a properly informed and considered decision by the Minister. It seems manifestly inadequate. There was no written advice on relevant risks. There was no information on how intelligence sharing would proceed: nothing, for example, to explain it would include both analytical products and raw data; nothing about any automated or bespoke arrangements (such as the capability).

60. The intelligence sharing authorisation in effect at the time of the decision to host the capability stood, nonetheless, and it permitted the GCSB to share intelligence with the foreign partner without qualification as to content or means. I do not find therefore that hosting the capability required further express Ministerial approval. It follows that hosting the capability without such approval was not unlawful.

61. I have no hesitation, however, in finding it was improper for the Bureau to host the capability without putting the matter before the Minister. The GCSB's governing legislation at the time stated that "the performance of the Bureau's functions is subject to the control of the Minister". That expresses a fundamental principle of accountable government. Briefing the Minister on the proposal to host the capability would have enabled the Minister to exercise control. Not briefing the Minister was not just a failure to observe the "no surprises" convention. It was a failure to respect and facilitate the control the Minister was entitled to exercise over the GCSB.

62. Seeking the Minister's approval would have required the Bureau to explain the legal and policy concerns that had been raised regarding the capability and how they would be mitigated by the terms of the proposed MOU (if that was the analysis). It would have enabled the Minister to consider whether to consult Cabinet colleagues, or even to seek a Cabinet mandate. Neither was beyond the realms of possibility. Both were precluded by the GCSB improperly keeping the decision to itself.

63. The GCSB now operates under a Joint Policy Statement on International Agreements and Arrangements, which sets out an expectation that an international agreement that deals with new policy should be approved by the Minister responsible for the agency.[8] I will return to this later, but note here that in my view this comes closer to the respect for Ministerial control that should have guided the decision to host the capability. It could also bring information about novel arrangements into the authorisation process for intelligence sharing, in contrast to the uninformative process followed when the capability was under consideration.

[8] JPS – 026 International Agreements and Arrangements at [40].

Should the IGIS have been notified?

64. The IGIS at the time was not notified of the decision to host the capability, despite Mr Murdoch suggesting this and another staff member identifying that there may be "oversight concerns" with the capability.

65. I consider that notification of the IGIS would have been appropriate for similar reasons to those for briefing the Minister. Hosting the capability was clearly a matter of significance for oversight.

FINDINGS

66. I find, in relation to the Bureau's decision to host the capability:

66.1. The GCSB undertook a reasonably robust investigation into the capability and the potential issues with hosting it. This included consulting the partners, which resulted in potential concerns being raised by GCSB staff about the operation of the capability in New Zealand.

66.2. When considering hosting the capability, the GCSB identified legal and policy concerns, including the potential for the capability to be used to support military operations. These concerns were circulated at the most senior level of the GCSB.

66.3. The record-keeping of the decision process was poor and there are significant gaps, which have made it difficult to identify reasons for certain decisions, particularly whether concerns about the capability were thought to be mitigated by terms in the MOU or were not borne out. There appears to be no substantive written legal advice, despite the GCSB's General Counsel being involved throughout the process.

66.4. Despite the then acting Director-General anticipating that the Minister responsible for the GCSB would be informed about the capability and possibly asked to approve GCSB hosting the system, this inquiry found no evidence of the Minister being told about the capability

66.5. The decision to host the capability on the terms set out in the MOU was significant, particularly given the potential uses of the capability to support military operations. It was a matter the Minister might have considered putting to Cabinet or selected Ministers. The Bureau should have briefed the Minister in accordance with the "no surprises" principle.

66.6. Though the authorisation process for intelligence sharing at the time seems manifestly inadequate, a Ministerial authorisation in place in 2012 for the GCSB to share intelligence and cooperate with the foreign partner was broad enough to cover the capability and so the decision to host the system without further Ministerial approval was lawful.

66.7. It was improper, however, for the GCSB to decide on hosting the capability without bringing it to the Minister's attention. By doing so it failed to respect and enable Ministerial control of the agency.

66.8. It would have been prudent for the GCSB to notify the IGIS at the time of the decision to host the capability.

HOW THE CAPABILITY OPERATED AT GCSB

67. Hardware for the capability was installed at a GCSB facility in 2012. The exact date is unclear, but a GCSB presentation in March 2012 advised that installation was planned for June. A presentation dated November 2012 referred to the capability having been delivered, with a training plan in progress. An engineer at the host facility emailed colleagues In November 2012 advising that the capability was about to be tested.

68. In early 2013 a GCSB officer emailed colleagues that overseas partners had started tasking the capability.

Terms of the MOU for the operation of the capability

69. As noted earlier, the MOU stated that any foreign government system operated in New Zealand or through its assets would operate "with the full knowledge and concurrence of the New Zealand Government". It added that:

> The operation of the capability's collection and processing suites […] must at all times be compliant with the Government Communications Security Bureau Act 2003 and other relevant New Zealand law […].[9]

70. The MOU went on to note that the capability would not be used to target a New Zealand citizen or permanent resident; no communications would be collected from the New Zealand telecommunications network without a warrant; and collection of communications would be strictly limited to collection of metadata.

71. The MOU provisions for control of the capability were:

71.1. Overseas partners would coordinate the use of the capability with the GCSB and would email requests for changes to the settings of the capability to be made by the GCSB.

71.2. For tasking of the capability, the GCSB would be notified by email and the GCSB would only respond if they did not concur with the tasking. If the GCSB did not concur, then the tasking would not be carried out.

71.3. Data provided by the GCSB would be deleted within one year.

---

9 MOU paragraphs III/A and B.

71.4. The GCSB would have a consolidated list of all current and planned collection activities.

71.5. At all times GCSB would have administrative access to the capability and would be provided training and instructions for identifying collection and tasking activities on the capability.

72. Key provisions of the MOU for GCSB to monitor operation of the capability were:

72.1. GCSB was to have system-level access to the capability and "at any time" have access to the results of any tasking of the capability.

72.2. GCSB would know how the capability was operating at any time;

72.3. GCSB would be notified and approve of any changes to the "type" of collection and/or target set beyond what was agreed in the MOU.[10]

72.4. GCSB would have access to the databases populated by the capability.

72.5. GCSB would be able to check all collection requests for compliance and have the authority to disapprove any such request for which compliance could not be affirmatively established.

73. The MOU included a provision that it would be reviewed no later than 24 months after the capability started operating, and then every three years thereafter. Both parties were responsible for the review.

74. My inquiry did not find any GCSB policies or procedures applying to the operation of the capability.

75. By contrast an overseas partner agency that also hosted the system had established detailed processes for its operation, specifying roles and responsibilities to review, approve and carry out tasking. GCSB officials had identified when deciding to host the capability that similar processes would be necessary for GCSB.

How the capability operated in practice

76. GCSB records of the operation of the capability during this period are patchy and many of the staff that dealt with its operation are no longer with the GCSB. This made it difficult to obtain full and clear information about how the capability operated.

Tasking

77. Most of the available operational records are email requests for "feed changes" to the settings controlling which GCSB-collected signals the partner system would acquire. Because these changes were generally necessary to enable a task they can be assumed to

[10] MOU paragraph III/C3

correlate with tasking. The requests indicated when tasking was being attempted, but not their purpose or justification.

78. The Bureau reported internally in February 2020 that the capability had been "rarely tasked - eight times in the past two years". These records had been obtained from the partner agency controlling the system. Seven of those tasking requests had been by GCSB and one by an overseas partner. The Bureau noted it had been unable to get tasking records dating back further than two years from its overseas partners due to a "system upgrade".

79. My search of GCSB email records found 29 requests for changes to be made to the settings of the capability (likely indicating tasking) between 2014 and 2020, in addition to the eight tasking instances identified by the GCSB.

80. All the requests appear to have been actioned by GCSB.[11] Only one included information about the purpose of the related tasking. None appeared to involve any questioning or investigation by GCSB of the purpose of the request.

81. Alongside the email requests, further details of tasking could be found in some GCSB monthly report documents from 2013 and 2014. These identified 22 further instances of tasking of the capability. Feed change requests corresponding to all of these instances of tasking were not found. Searches for this inquiry did not find all monthly report documents for the relevant period, so it is possible that this does not represent the full extent of reported tasking.

82. In total my inquiry identified at least 45 apparent instances of the capability being tasked.

83. The requests found by my inquiry do not however appear to represent the full history of tasking of the capability. My inquiry found several records of comments in emails by GCSB staff about high volumes of data being sent from the capability at times when there were no records of emails advising of the tasking or requesting feed changes. The implication is that GCSB staff were not always aware the capability was being tasked until after the fact.

84. If not for system issues with dataflow, there would apparently have been nothing to alert GCSB that these activities had occurred. This naturally raises the question of whether other tasking occurred without the knowledge of the GCSB, with no system issues to signal it.

85. It appears possible also that a request to change the settings of the capability might have been followed by multiple taskings. This was suggested by internal email noting the lack of input the GCSB had to the process and that a data flow arrangement should make the process invisible to the GCSB. This email noted that there was no need for the GCSB to monitor the dataflow.

[11] In one case it was unclear if any data was received by the other party.

86. From my review of the records, it appears possible that regular tasking could have been carried out without the need for any requests for feed changes, due to the availability of other information to overseas partners. It is difficult to draw any firm conclusions on this.

87. The lack of clear knowledge in GCSB of the tasking of the capability is in stark contrast to the MOU provisions for the GCSB to have full knowledge of its operation. This inquiry found no evidence of substantive due diligence being done by GCSB on the reasons for tasking of the capability while it operated. On only one occasion is there a record of the purpose of a particular tasking. The Bureau apparently neither received nor sought any information about what GCSB-collected data acquired by the system was going to be used for.

88. When asked about this in the course of the Inquiry, the GCSB noted:

> "GCSB is usually aware that [an overseas partner] is using data shared with it by way of [requests for changes to the capability's settings]. In the unlikely but possible situation no […] change was required, GCSB would only be aware that the data could be used by [an overseas partner], not that it had been."

89. Nor does there seem to be any way to acquire information about tasking retrospectively. Some records indicate tasking requests could issue through certain overseas partner systems, but the GCSB has been unable to provide records from these systems. Additionally, an update of an overseas partner system apparently made details of tasking through that system before 2019 unavailable.

90. In the circumstances I do not see how the Bureau could be sure the tasking of the capability was always in accordance with Government intelligence requirements, New Zealand law and the provisions of the MOU.

Access for GCSB to the results of the capability's tasking

91. The MOU provided for the GCSB to have access to the results of the capability through overseas systems. The GCSB advised in response to my inquiry, however, that it did not use these systems for access to any results of the capability. Nor was it aware of any consolidated list of results.

92. As a result, it is not clear how many taskings were successfully carried out as a result of the operation of the capability at GCSB. Possibly the GCSB might still be able to request this information. It appears, however, that the access agreed in the MOU is not currently in place. It is unclear whether it ever was.

Training, support, or guidance for operational staff

93. The GCSB put no policy or procedure in place, when the capability was installed, to guide operational decision-making. The only internal guidance documents produced dealt with the technical operation and security of the system, not compliance with the law and the terms of the MOU.

94. Emails from the time indicate that staff, particularly in the early years of operation of the capability, were unsure about how tasking requests should be handled. Many emails from staff dealing with these requests showed confusion about what was expected of them. This included GCSB staff having to ask an overseas partner agency for explanations and a copy of the MOU the GCSB had signed.

95. My inquiry found no guidance or instructions provided to these staff from the GCSB. The only training provided appears to have been from the overseas partner agency. Comments in emails suggest GCSB staff were under the impression they were meant to comply with requests from the overseas partner and not ask any questions. For example:

> […] we have no input whatsoever into the process as its all controlled from [overseas] […] [A staff member] has set up a separate data flow for the capability traffic so the process should be totally invisible to us.

96. Instructions to GCSB staff focused on the technical requirements of the capability (ie how to make sure it worked).

GCSB leadership knowledge of the capability

97. Senior GCSB staff and the Bureau's legal team apparently had little to no knowledge of the capability during its operation. I have seen no evidence of it being considered at this level after the lead-up to the signing of the MOU.

98. The capability was "rediscovered" at a senior level following concerns being raised about a separate GCSB system in 2020. The capability therefore appears to have operated largely without internal oversight following its approval. This includes a lack of consideration of it when the GCSB applied for authorisations for relevant signals collection activities, as discussed later.

Monitoring and review

99. My inquiry found no records of any GCSB audits of the operation of the capability. The only scrutiny of it was for certification, an assessment of conformity with technical standards.

100. I found no records of any checks by the GCSB of whether data was deleted as per the MOU, or to ensure that no New Zealanders' data was included as part of the capability's analysis.

101. The MOU was never reviewed and I found no records to suggest why not. A review would have been a check on whether the agreement was being executed. It could have alerted the GCSB leadership to the apparent disparity between what support for the capability was meant to involve and what was happening in practice.

Did GCSB receive and action requests to redirect collection for the capability?

102. The GCSB advised my inquiry that the capability only took selected data ("feeds") from signals collected by GCSB for its own, authorised purposes. My inquiry raised the question,

however, of whether it also involved the foreign partner requesting changes in collection to meet the purposes for which the capability was tasked.

103. My inquiry found records of feed change requests to the GCSB that included the foreign partner agency specifically asking for different collection to occur. Most feed change requests did not include details of the collection that was being sought.

104. There are no definitive records showing that GCSB collection was redirected in response to such requests, however. GCSB responses to feed change requests would simply confirm that feeds had been changed, with no indication of whether collection had also changed.

Was the capability at GCSB used to support military operations?

105. While it is clear that data supplied to the partner system in some parts of the world was used to support military operations, my inquiry was unable to determine whether military action was supported by any tasking of the capability at GCSB. With only one exception the available records include no information about the purpose of any individual tasking of the capability at GCSB. Although the potential for the capability to support military operations was flagged within GCSB several times, very clearly, before the decision to host the system, there was apparently no attempt to monitor whether this occurred in practice. I found no records of GCSB seeking any explanation for any tasking requests received.

106. Given the scope of GCSB signals collection it is less likely that GCSB data was used to support military action than was the case for data from other sources. It cannot however be ruled out. The possibility was recognised within GCSB. It remains a key issue in relation to the decision to host the system, regardless of the difficulty in verifying whether it came to pass.

Findings

107. I find that the capability operated at GCSB:

107.1. without adequate record keeping;

107.2. without due diligence by GCSB on the capability tasking requests;

107.3. without full visibility for GCSB of the capability tasking;

107.4. without adequate training, support or guidance for GCSB operational staff;

107.5. with negligible awareness of the capability at a senior level within GCSB after the signing of the MOU;

107.6. with no apparent access for GCSB to the outcomes of the capability's operation at GCSB;

107.7. without any auditing;

107.8. without the required review of the MOU;

107.9. without due attention to the possibility, recognised within the Bureau, that support for the capability could contribute to military targeting; and

107.10. without clarity, in consequence, as to whether data supplied by the GCSB to the capability did in fact support military action.

108. I note that the risk of GCSB support for the capability contributing to military action was moderated significantly by the geographical limits of GCSB collection. However, I find that the way in which the capability was operated meant that the Bureau could not be sure the tasking of the capability was always in accordance with Government intelligence requirements, New Zealand law and the provisions of the MOU.

WAS THE OPERATION OF THE CAPABILITY AUTHORISED?

109. While the capability was operating, the GCSB need to maintain authorisation for:

109.1. the sharing of GCSB intelligence with foreign partners through the capability; and

109.2. the signals collection that would provide the data needed for the capability.

Authorisation for sharing intelligence to the partner system

110. I have already found that the data sharing involved in hosting the capability was within scope of the broad Ministerial authorisation in effect in 2012 for sharing intelligence.

Sharing authorisations under the GCSB Act from September 2013

111. The law governing authorisation of intelligence sharing changed slightly in 2013, when the GCSB Act 2003 was amended. A new section 8B of the GCSB Act 2003 provided for the Bureau, in performing its intelligence gathering function, to provide "any intelligence gathered and any analysis of the intelligence" (rather than "reports on foreign intelligence") to authorised parties.[12]

112. The GCSB provided slightly more information in support of its first request for authorisation under the amended legislation than previously. There was no reference to the capability or any other particular mechanism by which intelligence would be shared.

113. The authorisation signed by the Minister was a brief statement of permission to share intelligence with listed entities, including the relevant foreign partner agency.

114. A subsequent application and authorisation in October 2014 were nearly identical. These authorisations were not for a fixed term and therefore remained in effect for subsequent years.

---

[12] GCSB Act 2003, s 8B(1)(c).

Sharing authorisations under the ISA

115. From 2017 the ISA also required the GCSB to have a Ministerial authorisation for sharing intelligence.[13] A Ministerial authorisation to share intelligence with relevant parties was issued on 18 September 2017. In it the Minister authorised the listed parties:

> 1. […] to receive from the Government Communications Security Bureau intelligence and analysis collected in accordance with the Government's priorities, pursuant to s10(1)(a) of the ISA.

116. The authorisation was subject to the GCSB complying with the Joint Human Rights Risk Management Policy before providing any intelligence and analysis to any authorised parties. It did not state any further conditions or any details of how intelligence would be shared.

117. In 2020 the GCSB sought and received another authorisation of the same scope and terms.

Analysis of authorisations to share intelligence

118. Like the authorisation for intelligence sharing in effect when the GCSB decided to host the capability, the succeeding authorisations under the GCSB Act and the ISA were broad enough to cover the operation of the capability. The provisions of the legislation or the Ministerial authorisations did not change sufficiently to require any separate authorisation or consideration of the system. I find therefore that the sharing of data through the capability was authorised and lawful.

119. I note however that the Ministerial authorisation under the ISA was subject to the condition that the GCSB comply with the Joint Human Rights Risk Management Policy before sharing any intelligence. The foreign partner was an "approved party" under the JPS "Human rights risk management", which meant the GCSB could provide information to it without approval for every instance of sharing, unless there was a "specific indication" that providing information would contribute to a breach of human rights. A "specific indication" was "specific and reliable information that one or more relevant parties could seek to take actions that cause such a breach in the particular circumstances".

120. My inquiry has found that the GCSB operated the capability without conducting any due diligence of when it was tasked. The inquiry was only able to find one instance where an instance of tasking included information about what the tasking was for. Moreover the understanding was that GCSB would accept tasking of the capability by default. It is not apparent therefore how the GCSB could have detected whether any "specific indication" of a risk of human rights breach might have arisen.

121. I therefore consider that, while the sharing of intelligence with the foreign partner through the capability was within scope of Ministerial authorisations, the GCSB's operation of the

[13] Section 10(1)(b)(iii).

capability, by failing to have processes to consider tasking requests, was inadequate to comply fully with the Ministerial authorisation.

Authorisations for signals collection relevant to the capability

122. This inquiry found no record of any consideration, before or during the GCSB's hosting of the capability, of how the supply of GCSB data to the system would relate to subsequent GCSB authorisations for relevant signals collection. The first substantive consideration of this was the GCSB's Chief Legal Adviser's briefing to the Director-General about the capability on 23 February 2021, after the system had ceased operating.

123. Over the period in which the capability operated, the relevant GCSB collection was authorised:

123.1. until 27 September 2013, by "standing authorisations" issued by the GCSB Director under section 16 of the Government Communications Security Bureau Act 2003 (the GCSB Act 2003);

123.2. from 27 September 2013, by five authorisations under the amended GCSB Act 2003;

123.3. from 3 September 2018, by five warrants, issued under the Intelligence and Security Act 2017 (ISA).

Standing authorisations prior to September 2013

124. Before 27 September 2013 "standing authorisations" were provided by the Director of the GCSB under section 16 of the GCSB Act 2003. The activity concerned with the capability was within scope of s 16.

125. "Authorisation" under s 16 was a delegation of a statutory power, not a warrant. There were no applications for s 16 authorisations. It appears that it was GCSB practice that a standing authorisation was approved when a Director took office and remained in effect until that Director resigned, after which the new Director would sign a new standing authorisation.

126. There were two standing authorisations covering relevant GCSB activities while the capability was operating. One was issued by Simon Murdoch on 5 July 2011 and one by Ian Fletcher on 7 February 2012.[14] The two authorisations were identical.

127. When the capability began operating, therefore, the Director of the GCSB was empowered by s 16 to carry out the underpinning activities, which was executed by GCSB staff delegated by a "Director's authorisation".

[14] Mr Fletcher advised the inquiry that the authorisation was signed four days after he started at the GCSB.

Authorisations from September 2013 under the amended GCSB Act 2003

128. From September 2013 the relevant GCSB collection was authorised under an amended s 16 of the GCSB Act 2003, which provided for the Director to authorise GCSB staff to undertake interception activities under certain conditions.

129. Authorisations under the amended s 16 remained instruments for delegating the Director's statutory power to undertake certain activities without warrant. Unlike the earlier standing authorisations they were issued by the Director in response to applications.

130. None of the applications for authorisations mentioned the capability. When asked if the capability was considered in the context of an application, the GCSB advised it did "not yet have documents to demonstrate that it was considered, but we expect it may have been". This inquiry found no information to support this.

131. The applications for these authorisations noted that authorised activities could be done to meet requests from certain foreign partners as well as to share intelligence gathered. Activities under these authorisations could be carried out for the purposes set out in section 8B of the GCSB Act. One of these purposes was to gather and analyse intelligence about information infrastructures. The definition of "information infrastructure" was broad enough to encompass the purpose of the capability.

Authorisations from September 2017 under the GCSB Act

132. The last authorisation under the GCSB Act was issued by the Minister under s 15A, rather than a s 16 authorisation from the Director. From this point, therefore, the GCSB was under a duty of candour when applying for an authorisation. This requires the applicant to inform the decision-maker "clearly and transparently" of all "material facts".[15]

133. The authorisation permitted interception of signals of the type relevant to the capability, for purposes including intelligence gathering.

134. The application noted the expected value of collection in obtaining intelligence about information infrastructures, but did not refer to the specific outputs of the capability. The authorisation noted that the Bureau would share relevant intelligence with certain foreign partners. The application explained controls on partner use of such data, but in terms reflective of uses other than the capability. A section on risk addressed only the risk of a foreign government identifying the specific target of an operation.

135. As for the preceding authorisations, this authorisation covered activities in terms abstract enough to encompass the collection and sharing involved in supporting the capability, but with no mention of it specifically or the type of activity supported and its possible purposes.

---

[15] Re X 2016 FC 1105 at [107] to [108]

Intelligence warrants from September 2018

136. Following the enactment of the ISA Act 2017, the relevant type of GCSB signals collection was authorised by intelligence warrants.

137. The relevant provisions of the warrants were substantially similar over the period. None of the warrant applications referred to the capability or its primary output. The GCSB has also noted that the capability was not referred to in drafting instructions for the warrants.

138. The proposed activities under the warrants included a category of activities what broadly covered the outputs of the capability and provided for the sharing of the results of the capability with certain foreign partners, as well as conducting activities at the request of foreign partners and passing on the results.

The GCSB analysis of relevant authorisations

139. In February 2021, the GCSB's analysis of whether the capability had been properly authorised focused on the last relevant warrants and stated that:

139.1. the provision of collected data to the partner system had fallen within one of the purposes of the warrants;

139.2. the use of data by the capability had complied with the conditions of the warrants because the key definitions referred to a relevant kind of use; and

139.3. sharing the results of authorised activities was addressed explicitly in the warrant application.

140. The Bureau's overall conclusion on authorisation was that the operation of the capability had been "within scope of the … activities authorised" under the warrant.

141. The Bureau also considered it had met its duty of candour in the warrant application by presenting the material facts, regardless of the fact that the capability was not mentioned.

142. The advice noted however that it would be "an improvement" to refer specifically to "this particular instance of intelligence sharing" if and when another warrant was sought.

Analysis of collection authorisations

143. As the capability was a data sharing mechanism, not a collection activity, it was not and could not have been directly authorised by the authorisations the GCSB was required to seek for its relevant signals collection. The key questions regarding the authorisations are whether they covered the collection activities that would support the capability and whether the applications were sufficiently candid on the facts relevant to that activity.

144. Predominantly the capability would receive signals from collection being undertaken by GCSB in accordance with its function of gathering intelligence in accordance with New

Zealand Government requirements. The relevant authorisations were focused on collection to meet those requirements.

145. The MOU for the capability apparently contemplated, however, that GCSB might also respond to requests for specific collection from the foreign partner rather than sharing already collected data.

146. There were also indications from GCSB staff that supporting the capability could involve redirecting collection, but a lack of any records showing that this occurred. GCSB responses to feed change requests would simply confirm that feeds had been changed. On the records available my inquiry could not determine whether collection changes occurred alongside this.

147. Regardless of whether collection changes at the behest of the foreign partner actually occurred, if they were anticipated as part of hosting the capability they had to be provided for in the relevant collection authorisations.

148. The only limitation on the purpose of collection under the "Director's authorisations" in effect when the capability began operating was that it was to obtain "foreign intelligence".[16] The statutory objective of the Bureau at the time, moreover, included providing foreign intelligence "to meet international obligations and commitments of the Government of New Zealand".[17] Those authorisations were broad enough therefore to cover the activities that would support the capability, even if that was to include changing collection at the request of the foreign partner.

149. The same applies to the succeeding authorisations under the GCSB Act and the intelligence warrants under the ISA, which provided for conducting activities at the request of partners and passing on the collected information.

150. I find therefore that the collection authorisations in effect while the capability operated were broad enough in their terms to cover the activities that would provide data to the capability, even if that was to include altering collection to meet a request from the foreign partner.

151. I find also that the GCSB met its duty of candour where that applied, when seeking the collection authorisations under which the capability would operate. This is essentially because the material facts were those relating to the collection activity – ie its scope, purposes and value. The applications for the relevant authorisations and warrants covered these aspects of the activity.

152. The facts about the capability that made it significant were material to the original decision to host it, ie the decision to share collected data. Had the GCSB properly brought the capability to the attention of its Minister in the first place and received assurance that hosting it was in accordance with the Government's wishes (whether on the terms in the

[16] GCSB Act 2003, s 16(2)(c).
[17] GCSB Act 2003, s 7(1)(b).

MOU or any other conditions) it could have referred to it in applications for authorisations as relevant contextual information. To that extent I agree with the GCSB that mentioning it would have been an improvement to the warrant applications. Mentioning it would not have achieved anything more, however. The collection authorisations could not remedy the earlier failure.

153. I have one further observation to make. There is one scenario contemplated by the MOU that I have no doubt would have been outside the scope of the various collection authorisations and, therefore unlawful and improper. Action from GCSB on a request from the partner operating the capability to collect signals not already tasked by GCSB, for the purpose of supporting a military operation, would have been outside the scope of the stated purposes of the authorisations. I would hope this never happened but, given the inadequacies in the GCSB's monitoring and record keeping of the capability in action, I have no comfort that it did not.

Findings

154. I find that the collection authorisations in effect while the capability operated were broad enough in their terms to cover the signals collection that provided data to the capability, even if that was to include altering collection to meet a request from the foreign partner, unless that request was for the purpose of supporting a military operation.

155. I find that the GCSB met its duty of candour when seeking authorisations while the capability was operating. The material facts in relation to those operations concerned the collection of signals rather than the subsequent sharing of them with the partner agency through the capability.

IS THERE A RISK THE ISSUES WITH THE CAPABILITY COULD RECUR?

156. The inquiry has found failings in the decision-making process for hosting the capability, in managing its subsequent operation, and in how it was authorised throughout its operation. The Bureau's support for the system has come to an end, however. The GCSB no longer contributes to the capability and the equipment has been removed. The obvious question is whether my findings have ongoing significance. Is there a risk that the shortcomings in the GCSB's involvement with the capability might be repeated?

157. The Bureau, its operations, its governing statute, its policies and compliance systems have changed significantly over the period in which the capability operated, and since. The agency has grown in size and in the sophistication of its administrative systems. It has become accustomed to operating under more rigorous statutory requirements, including a new authorisation regime. It has a new framework for entering into international arrangements. From having a single senior legal counsel at the time of the decision to host the capability it now has a substantial legal team. Its record keeping systems and practices (while still not without issues) have improved. Its audit and compliance teams and practices have developed. Oversight from my office has developed substantially.

158. I think these developments have reduced the risk that the shortcomings I have identified in the Bureau's hosting of the capability might recur today in a similar situation. This inquiry might also have an effect.

159. I consider it less likely now that a matter with such sensitivities would be identified as requiring Ministerial attention, but then omitted from the Ministerial agenda without explanation or any apparent reason. I am mindful, however, that the failure in relation to the capability occurred in a transition between Directors. Such transitions are likely to remain a vulnerable point, as they do for any agency.

160. I also consider it less likely that the Bureau, after having entered an agreement with a partner agency, would implement it as poorly as it implemented the MOU for the capability.

161. In July 2021 the GCSB and the NZSIS finalised a Joint Policy Statement (JPS) on International Agreements and Arrangements. The JPS requires both agencies to keep a centralised register for foreign cooperation arrangements, which I had previously recommended. An arrangement is defined as "non-binding, with no legal consequences", reflecting "a political commitment only". It seems to me that any future agreement for GCSB to host a partner system such as the capability (a system controlled substantially by the partner) would count as an international arrangement, triggering the JPS requirements.

162. Those requirements include:

162.1. all international arrangements must have an assigned "business owner" and a subject matter expert responsible for negotiation, management and the relationship or form of cooperation established by the instrument;

162.2. legal and policy teams must be made aware of the arrangement;

162.3. ensuring the signed agreement is stored in the agency register;

162.4. the Ministry of Foreign Affairs and Trade must be consulted at an early stage;

162.5. all arrangements must be approved and signed by the Director-General or delegate, or the Minister where the arrangement involves new policy.

163. My intention in recommending a register was to facilitate oversight of international arrangements by my Office as well as agency leadership and compliance staff. Had the MOU on the capability been registered its execution might have received more attention from the Bureau and been visible for oversight.

164. A centralised register would provide an important oversight safeguard in the existing system for such cooperation. It would have expedited the Bureau being able to respond to my question about other partner systems operating in New Zealand.

RECOMMENDATIONS

165. Determining appropriate recommendations for this inquiry has required careful consideration and discussion with the GCSB. I consider that the below recommendations, the organisational developments at the GCSB, the findings of this report, and continued monitoring by my office will help to address the risk of similar issues arising.

166. I recommend that the GCSB:

166.1. produce internal guidance to reflect existing requirements that international agreements and arrangements of significance are consulted with the Minister;

166.2. compile a register of collection or analysis capabilities in New Zealand that are operated by foreign partners;

166.3. undertake an audit of its systems, including any foreign partner capabilities. I note that this is already underway;

166.4. initiate a programme of work to review and monitor international agreements and arrangements within specified timeframes; and

166.5. establish processes which enable my office to view new international agreements and arrangements when entered into.

167. The GCSB has agreed to all recommendations.