Office of the Inspector-General of Intelligence and Security

Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009-2015

Public Report

Cheryl Gwyn
Inspector-General of Intelligence and Security

4 July 2018

CONTENTS

Introduction 4

Procedure 5

Terminology 6

Guiding questions 6

Key findings 7

Outcome 8

The conduct of signals intelligence by GCSB 10

The law governing the GCSB 10

Authorisations for interception 10

Meaning of communication, private communication and interception 12

Prohibition on targeting the private communications of New Zealanders 13

Prohibition on targeting privileged communications 14

Duty to minimise impact on third parties 14

Requirement for destruction of irrelevant records obtained by interception 14

Government's foreign intelligence requirements and priorities 14

Lawfulness of particular collection methods 15

GCSB policies 16

Private communications of New Zealanders 16

Privileged communications of New Zealanders 19

Minimising impact on third parties 20

Retention and destruction of intercepted communications 21

Partner collaboration and information sharing 22

Internal compliance auditing 22

GCSB SIGINT processes 23

Collection requirements 23

Authorisation 24
Tasking 24
Collection 24
Analysis 25
Reporting 25
Data retention 26
Data sharing 26
Auditing & Compliance 26
SIGINT Production Cycle 26
GCSB Activity in relation to the south Pacific 2009-2015 27
Context 27
General findings 28
Findings regarding complainants' communications 29
Findings regarding GCSB compliance procedures and systems 30
Glossary 31

INTRODUCTION

1. This report covers:

   1.1. an inquiry into several individual complaints against the Government Communications Security Bureau (GCSB) prompted by reports of GCSB foreign intelligence activity in relation to the South Pacific between 2009 and 2015; and

   1.2. a review of the relevant Bureau compliance procedures and systems during that period.

2. In March 2015 there was extensive news media coverage of what were alleged to be classified United States National Security Agency (NSA) documents disclosed by Edward Snowden. These purported to show evidence of intelligence activity by the GCSB in the South Pacific. The news coverage included a radio interview with the former GCSB Director Sir Bruce Ferguson, who acknowledged that New Zealand had an interest in the South Pacific and described the Bureau's business as involving "mass collection" or "full take collection" of communications.[1] In consequence of the media coverage I received several complaints.

3. Some complaints were from people who believed they might have been subject to or affected by the alleged GCSB activity. I have jurisdiction to inquire into complaints from people who have or may have been adversely affected by any action of the GCSB.[2] I began an inquiry into those complaints, relating to alleged GCSB communications surveillance activities in several Pacific Islands nations, on that basis.

4. Other complaints were against the alleged conduct of the GCSB generally. These did not assert any adverse effect on the complainants and were therefore not within my complaints jurisdiction. I have a broad jurisdiction, however, to review the compliance procedures and systems of New Zealand's intelligence and security agencies.[3] I decided to review the Bureau's procedures and systems relevant to its activities in relation to the South Pacific during the period at issue: 2009-2015.

5. I am required to report publicly on every inquiry I undertake.[4] This is an important aspect of effective oversight and public accountability. However, I am not able to disclose publicly all of the information I obtained in this inquiry. I am barred by law from disclosing information that, if publicly disclosed, would be likely to prejudice the entrusting of information to the New Zealand Government on a basis of confidence; prejudice the continued performance of the functions of an intelligence and security agency; or prejudice the international relations of the

---

1 "GCSB in mass collection of Pacific data: Ferguson" *Radio New Zealand News* (online ed, 6 March 2015); Alastair Thompson "Former GCSB Director Admits to Mass Surveillance of NZers" *Scoop News* (online ed, 7 March 2015).

2 At the time of the inquiry covered by this report, this jurisdiction was provided by section 11(1)(b) of the Inspector-General of Intelligence and Security Act 1996 (IGIS Act). It is now provided by section 171(2) of the Intelligence and Security Act 2017 (ISA).

3 IGIS Act, s 11(1)(d); ISA, s 158(f).

4 IGIS Act, s 188.

New Zealand Government.[5] This precludes any disclosure of whether the GCSB undertook intelligence activity in relation to any particular persons or places in the South Pacific. I accept that any such disclosure would be likely to cause adverse effects on New Zealand's international relations. It could also undermine the efficacy of foreign intelligence collection by disclosing technological, logistical and other capabilities and/or limitations; and disclose information provided in confidence by other governments.

6. I am, however, committed to providing as much public information about national security activities as I can, within the limits of my responsibilities. To that end I withhold from my public reports information only where and to the extent that I am satisfied disclosure would prejudice the national interests that I am required by law to protect. If I identify unlawful or improper conduct or inadequate procedures or safeguards, I expect to be able to make that public, even if it is necessary to withhold information about the specific subject-matter. In particular I expect to be able to disclose any instance of unlawful conduct affecting a complainant.

7. In the interest of informing the public I describe in this report, to the limited extent possible, the foreign intelligence capabilities available to the GCSB during the relevant period and how they were used. My review of the policies and procedures of the time is essentially a historical survey: the relevant legislation has since changed substantially and the associated policies and procedures have largely been superseded.

PROCEDURE

8. The complaints I received alleging an adverse impact on the complainants were from individuals concerned that their communications were or could have been intercepted by the GCSB during work or travel in various countries in the South Pacific. Some of these complaints did not proceed, at the complainants' request.[6] Others, as noted above, did not allege any adverse impact on the complainant and therefore were not investigated. They were however taken into account in deciding the scope and direction of my review of GCSB procedures and systems safeguards.

9. On 7 April 2015 I advised the then Acting Director of the GCSB, Una Jagose, of the scope of my inquiry and review and sought relevant information. In response and over the course of the inquiry, my office obtained information from GCSB records and staff, including those involved in intelligence-gathering and those with responsibility for analysis and dissemination of intelligence reports. We examined GCSB policy and procedure documents that were in effect over the relevant period. We also conducted independent searches of GCSB records. I

---

5 ISA, s 188.

6 I sought the consent of each complainant for two reasons. First, I am obliged to notify the Director of the GCSB of any complaint before proceeding to an inquiry. Second, the inquiry involved searches of GCSB records to check for any reference to each complainant and it was necessary to obtain their agreement before conducting those searches.

received full cooperation from the GCSB in the conduct of this inquiry and review. I am grateful to the GCSB staff who gave much of their time for this purpose.

10. In accordance with my statutory obligations, I provided a draft of this report to the Director-General of the GCSB in February 2018, to consult on factual accuracy; provide an opportunity for comment on any adverse statements;[7] and consult on the security classification of this report.[8] I have also sought the views of the Ministry of Foreign Affairs and Trade.

11. I am grateful for the professional and constructive approach the Bureau took to this process, particularly considering the extent to which this report provides information on its operation that it has not previously disclosed.

12. In addition to this public report I have provided a full, classified report to the Minister responsible for the GCSB and the Director-General of the GCSB. That report includes, in appendices, information that I am satisfied falls within the national security and related restrictions I must observe (see paragraph 5 above). Accordingly the appendices to the classified report are not included with this public report. This public report does, however, set out my findings in full. The classified report makes no findings or recommendations that are not recorded here.

13. I have also provided responses to each potentially adversely affected complainant, to the extent that I am able to do so within the applicable statutory constraints. I have not included the specific details of complaints and complainants in this public report, both for reasons of individual privacy and because those details are not critical to my overall findings.

TERMINOLOGY

14. Signals intelligence is a specialised, highly technical undertaking with its own vocabulary. This report uses plain language as far as possible but use of some specialised terms is unavoidable. These are generally explained as they occur, but a glossary of key terms can also be found at the end of this report.

GUIDING QUESTIONS

15. There was considerable overlap in the questions raised by complainants, in news media coverage and by my review. They can be summarised as follows.

16. During the period covered by this inquiry and review (2009-2015), regarding communications to and from the South Pacific:

    16.1. Was the content or metadata of any of the complainants' private communications intercepted by GCSB?

---

7 ISA, s 176(4).
8 ISA, s 185(6).

16.2. If intercepted, was the content or metadata of any of the complainants' private communications retained by GCSB?

16.3. If intercepted and retained, was the content or metadata of any of the complainants' private communications subsequently destroyed by GCSB?

16.4. If intercepted, was the content or metadata of any of the complainants' private communications provided by GCSB to any other person or agency?

16.5. If any such interception, retention, destruction or sharing occurred, was it lawful and proper?

16.6. If the GCSB undertook "full take" collection of communications, what did that mean?

16.7. What policies and procedures did the GCSB have in place for the purpose of ensuring any interception of private communications was conducted lawfully and properly?

16.8. What policies and procedures did the GCSB have in place to ensure compliance with the general prohibition in the GCSB Act 2003 on targeting New Zealanders' private communications? Was the GCSB's interpretation of "private communications" consistent with that general prohibition?

16.9. What policies and procedures did the GCSB have in place to ensure compliance with the legal constraints on targeting privileged communications?

17. In addition to the questions above, some complaints raised the question of whether the GCSB undertook "mass surveillance" in the South Pacific. This term was also frequently used in media coverage at the time.

18. "Mass surveillance," I find, lacks a clear and commonly agreed meaning. Rather than attempting to define it for the purpose of finding whether GCSB undertook it or not, I have undertaken in this report to describe the nature of the Bureau's activity, as far and as clearly as possible. In short I have sought to explain what the Bureau does, rather than use or dismiss a label that means different things to different people.

KEY FINDINGS

19. While I am unable to disclose specific information about particular intelligence-gathering or particular targets, I find as follows:

20. The GCSB undertook signals intelligence-gathering in relation to New Zealand's interests in the South Pacific during 2009-2015, including the collection of satellite communications.

21. There were statutory authorisations in place enabling the GCSB lawfully to collect signals intelligence in relation to New Zealand's interests in the South Pacific during this period. The GCSB had policies and procedures in place to govern its foreign intelligence activities, most of which were amended or replaced over the period in response to changes in legislation.

22. There is no evidence that GCSB acted outside the relevant authorisations and statutory prohibitions to any significant extent. This inquiry found two documented breaches, but these were inadvertent, were detected and remedied and did not indicate an institutional disregard for the relevant controls.

23. "Full take" was a phrase GCSB used to describe the storage of all communications data of certain types acquired from a particular satellite communications link, in pursuit of intelligence. Data stored from "full take" collection was "unselected", meaning it had not been filtered by reference to selectors (eg telephone numbers) before being stored. "Full take" collection contrasted with collection that resulted in storage of "selected" data, which had been filtered by reference to selectors.

24. There is no evidence that the GCSB deliberately targeted the private communications of any complainant for collection, or retained any data relating to any complainant.

25. It is possible that some of the private communications of some complainants were collected as part of interception activity, either inadvertently (by mistake), or incidentally, which means:

    25.1. in the course of using collection methods that did not target those individuals, but which inherently involved the acquisition of some non-targeted communications; or

    25.2. if those individuals had any communications with persons or organisations whose communications were being targeted for collection.

26. The likelihood that complainants' communications were collected inadvertently or incidentally ranges from zero to possible, considering variables of location, timing and the complainants' likely communication activity. If any such collection did occur, there is no evidence that GCSB retains any such data.

27. Some communications collected by GCSB in relation to the South Pacific were shared with its "Five Eyes" partner intelligence agencies ("partner agencies").[9] It is unlikely that any data relating to any complainant's communications has been shared with a partner agency, given the targeted nature of such sharing and access and the safeguards against unauthorised access to the private communications of New Zealand nationals. I cannot determine conclusively, however, whether any data relating to any complainant might still be held in systems administered by partner agencies.

OUTCOME

28. Somewhat unusually, I make no recommendations as a result of my inquiry and review. This follows from the absence of any adverse findings in relation to the complaints, and from the fact that the GCSB policies and procedures reviewed applied to operations under the GCSB Act

[9] The "Five Eyes" partnership is an intelligence-sharing arrangement between the United States, the United Kingdom, Canada, Australia and New Zealand.

2003 and have largely been superseded by new versions designed for compliance with the Intelligence and Security Act 2017. This inquiry and review will however inform my Office's ongoing review of all intelligence warrants issued to the GCSB and our further scrutiny of the Bureau's policies, procedures and activities.

THE CONDUCT OF SIGNALS INTELLIGENCE BY GCSB

29. The GCSB is a signals intelligence agency. The scope for it to lawfully intercept private communications is determined by its statutory framework.

The law governing the GCSB

30. Communications interception and analysis is, by its nature, highly intrusive. Intentionally intercepting private communications is ordinarily an offence.[10] The legislation governing the GCSB provides for it to collect signals intelligence lawfully, including under specific authorisation.

31. The principal legislation governing the GCSB during the period covered by this report was the Government Communications Security Bureau Act 2003 (the Act). The Act was amended part-way through the period by the GCSB Amendment Act 2013, which took effect from 27 September of that year.

32. The 2013 amendments were intended to clarify the parameters for the Bureau's activities.[11] There were changes to the GCSB's statutory objective, functions, powers and limitations. The Bureau's core functions – information assurance and cybersecurity, foreign intelligence, and co-operation with and assistance to other entities – were redefined.[12] The amendments made it clear that limits on the Bureau's ability to intercept the private communications of New Zealanders applied to its foreign intelligence function, but not to its information assurance and cyber security functions, or its function of providing assistance to other entities.

Authorisations for interception

33. The Act provided for two principal forms of authorisation for the Bureau to intercept communications: an interception warrant[13] and an access authorisation.[14]

34. In plain terms an interception warrant permitted the Bureau to intercept the communications of a person or persons, or communications to and from a place or places, where that would otherwise be unlawful. Until 2013 an interception warrant could be issued only for the purpose of obtaining foreign intelligence. Following the 2013 amendments to the Act a warrant could also be issued for information assurance and cybersecurity purposes. The amendments also provided for a warrant to be issued in respect of a class or classes of persons or places.

---

10 Crimes Act 1961, ss 216B and 252.

11 See the Explanatory Note to the Government Communications Security Bureau and Related Legislation Amendment Bill, at 2.

12 Sections 8A, 8B and 8C.

13 Section 17 before amendment; section 15A(1)(a) after amendment.

14 Section 19 before amendment; section 15A(1)(b) after amendment.

35. An access authorisation permitted the Bureau to access one or more "computer systems" (in the pre-amendment Act), or "information infrastructures" (in the amended Act) that it otherwise could not access lawfully. As with an interception warrant, until 2013 an access authorisation could be issued only for foreign intelligence purposes. The 2013 amendments enabled an access authorisation to be issued also for information assurance and cybersecurity purposes, and in respect of a class or classes of information infrastructures.

36. Until the 2013 amendments an interception warrant or access authorisation was issued by the Minister responsible for the GCSB. The amended Act required the involvement of the Commissioner of Security Warrants, with the Minister, in the issue of any warrant or authorisation under which anything might be done for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident.[15]

37. A warrant or access authorisation could be issued for up to 12 months.[16] The Minister, or Minister and Commissioner, had to be satisfied that specific criteria were met. These differed in their wording before and after the 2013 amendments, but consistently required in effect that the proposed interception or access was necessary for a statutory purpose or function of the Bureau and would be a proportionate use of its powers.[17] The issuing authorities could apply any conditions to a warrant or access authorisation they considered desirable in the public interest.[18]

38. Some interception could be undertaken without a warrant or access authorisation, on the authority of the GCSB Director.[19] A 'Director's authorisation' could (in effect) permit 'passive' interception of signals transmitted in free space on the electromagnetic spectrum, provided no New Zealanders' communications were targeted. The GCSB's two major signals interception stations – the high-frequency radio interception and direction finding station at Tangimoana, in Manawatu, and the satellite communications interception station at Waihopai, in Marlborough – operated during the period covered by this report under Director's authorisations.[20]

39. Through the 'Five Eyes' partnership, GCSB may also request partner agencies to carry out collection and may be granted access to information collected by those agencies.

40. Until 2013, the Bureau operated on the understanding that collection requests to partners and access to partner information were lawful without any need for authorisation, as the Act defined the Bureau's functions as including gathering foreign intelligence "by cooperating with public authorities or other entities in New Zealand and abroad."[21] The Bureau did not

---

15 Section 15B.
16 Section 22(1) before amendment; section 15D(1)(c) after amendment.
17 See sections 17(3) and 19(2) before amendment; section 15A(2) after amendment.
18 Sections 17(5) and 19(5) before amendment; section 15A(4) after amendment.
19 Section 16 before and after amendment.
20 Before 2013 a single authorisation covered both Tangimoana and Waihopai. After 2013 each was authorised separately.
21 Section 8(1)(a)(ii).

therefore seek warrants or authorisations for such requests or access, as a warrant was required only to intercept communications that were "not otherwise lawfully obtainable by the Bureau."[22]

41. The 2013 amendments to the Act defined the Bureau's functions in different terms. In particular the "cooperation" function noted above was removed from the Act without any equivalent replacement. In response to this and other changes the Bureau subsequently sought and received access authorisations to cover any collection requests to partners or access to their collected information.

Meaning of communication, private communication and interception

42. "Communication" was broadly defined under the Act to include "signs, signals, impulses, writing, images, sounds, or data that a person or machine produces, sends, receives, processes, or holds in any medium." The 2013 amendments added "information" to the list.[23]

43. A "private communication" was defined as follows:

> **private communication** –
>
> (a) means a communication between 2 or more parties made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but
>
> (b) does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so.[24]

44. Following the 2013 amendments a "privileged communication" was defined by reference to categories of privilege protected in court proceedings under the Evidence Act 2006: communications with legal advisers or ministers of religion, preparatory material for legal proceedings, and information obtained by medical practitioners or clinical psychologists.[25]

45. "Intercept" was defined as including "hear, listen to, record, monitor, acquire, or receive a communication, or acquire its substance, meaning or sense". "Interception device" meant "any electronic, mechanical, electromagnetic, optical or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept communications."

---

[22] Section 17(1).
[23] Section 4.
[24] Section 4. This definition was unchanged by the 2013 amendments.
[25] Section 15C of the Act cross references ss 54, 56, 58 and 59 of the Evidence Act 2006.

Prohibition on targeting the private communications of New Zealanders

46. Section 14 of the Act prohibited the Bureau, when collecting foreign intelligence, from undertaking any activity for the purpose of intercepting the private communications of New Zealand citizens or permanent residents (New Zealanders).[26] The narrow exception was where a New Zealander met the definition of a "foreign person" or "foreign organisation". Where that was the case – in effect, where it could be made out that a New Zealander was an agent of a foreign power – interception could proceed where a warrant or authorisation issued by both the Minister and the Commissioner of Security Warrants was in place.[27] No deliberate interception of the private communications of a New Zealander could be enabled by a section 16 Director's authorisation, whether or not they were assessed as an agent or representative of a foreign organisation.

47. Section 14 was headed "Interceptions not to target domestic communications" until 2013 and "Interceptions not to target New Zealand citizens or permanent residents for intelligence-gathering purposes" after the 2013 amendments. The terms of the section prohibited GCSB from taking actions "for the purpose of" intercepting the private communications of New Zealanders. The concept of "targeting" was important to the Bureau's understanding of the limitation imposed by the section. The question of whether a Bureau activity "targeted" a New Zealander was critical to any consideration of its lawfulness: in particular, whether the activity was done for the purpose of intercepting a New Zealander's private communications.

48. Under the 2003 Act, a legal question arose as to whether the communications of a New Zealander meant only the content of such communications, or included metadata about them. This was a matter of genuine uncertainty (recognised by Inspector-General Neazor, among others). It was ultimately resolved by the 2013 amendment of the definition of "communication" (see paragraph 42 above), which clarified that "communication" encompassed "information" (which was understood to include metadata).

49. The 2013 amendments also added a subsection (2) to section 14, which provided expressly that any incidentally obtained intelligence obtained by the Bureau in the performance of its intelligence gathering and analysis function was not obtained in breach of the section establishing that function (s 8B). Incidentally obtained intelligence was defined as (in effect) non-foreign intelligence acquired in the course of gathering foreign intelligence.[28]

---

[26] The Act did not define New Zealand citizenship, which is defined by the Citizenship Act 1977.

[27] Section 15B(1).

[28] Section 4. The definition in full read: "incidentally obtained intelligence means intelligence – (a) that is obtained in the course of gathering intelligence about the capabilities, intentions, or activities of foreign organisations or foreign persons; but (b) that is not intelligence of the kind referred to in paragraph (a)."

Prohibition on targeting privileged communications

50. From 2013 the Act expressly prohibited the issue of an interception warrant or access authorisation, or the exercise of any powers, for the purpose of intercepting privileged communications of a New Zealander.[29]

Duty to minimise impact on third parties

51. For any authorised interception, section 24 of the Act imposed a duty to minimise any impact on third parties. Those executing a warrant or access authorisation, or assisting, were required to "… take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting communications that are not relevant to the persons whose communications are to be intercepted."

Requirement for destruction of irrelevant records obtained by interception

52. Section 23 of the Act required the destruction, as soon as practicable after interception, of any intercepted communication (any copy of it, any part of it, and any record of the information obtained by the interception) except to the extent that the information in the copy or record related directly or indirectly to the Bureau's statutory objectives or functions.

Government's foreign intelligence requirements and priorities

53. Under section 8B of the Act the Bureau could collect foreign intelligence only in accordance with Government requirements.

54. My June 2017 report into GCSB's process for determining its foreign intelligence activity explained the system for establishing and implementing the Government's foreign intelligence requirements.[30] This system applied during the period addressed by this report.

55. In summary, the requirements were documented in the Foreign Intelligence Requirements (FIRs). These were approved by a committee of senior security officials (the Officials Committee for Domestic and External Security Coordination, or ODESC) and endorsed by the Cabinet Committee on Domestic and External Security Coordination. The FIRs most relevant to this enquiry were approved by ODESC on 11 February 2010.[31]

56. The FIRs identified subjects of intelligence interest and their relative priorities. They did not authorise particular foreign intelligence activity, but guided the allocation of resources across the range of foreign intelligence activities undertaken by the Bureau. There were several broad themes, with a requirements paper for each theme that identified related issues and

---

[29] Section 15C(1).

[30] Inspector-General of Intelligence and Security *Report into Government Communications Security Bureau's process for determining its foreign intelligence activity* (June 2017).

[31] Earlier FIRs, superseded by those approved in February 2010, also included requirements relevant to the South Pacific or with general application.

gave each a specified level of priority. The details are classified, but this inquiry did not identify any GCSB activities inconsistent with the FIRs in effect at the time.

57. From 2012 onward the FIRS were supplemented by more detailed National Intelligence Priorities (NIPs). These specified intelligence questions and/or lists of key groups related to specific issues set out in the FIR requirements paper. Again the details are classified. From 2015, the FIRS were superseded by National Intelligence Priorities, which are reviewed periodically.

Lawfulness of particular collection methods

58. The GCSB Act did not prescribe or prohibit any particular interception method. The lawfulness of any method employed by the Bureau therefore depended on how its particular features aligned with the Bureau's statutory powers and obligations as a whole, and with the terms of any relevant warrant or access authorisation.

59. Signals intelligence collection methods (including what the Bureau referred to as "full take" collection, which is addressed further under the heading "Collection" below) can result in the acquisition of irrelevant communications alongside those sought.[32] While the GCSB Act implicitly anticipated this possibility, it provided protections to ensure that irrelevant collection was minimised.

60. At the outset, the Act required the Minister (with, after 2013, the Commissioner, where relevant) to consider the "particular interception" proposed by GCSB and be satisfied, before issuing the warrant, that (among other things) "the value of the information sought to be obtained under the proposed warrant justifies the particular interception."[33]

61. Other protections included the duty to minimise the impact of interception on third parties (s 24 of the Act) and the requirement for destruction of irrelevant records obtained by interception as soon as practicable after the interception (s 23).

62. These provisions meant that collection resulting in the acquisition of irrelevant communications or otherwise impacting third parties would not be unlawful *per se,* so long as the Bureau met its corresponding obligations regarding the destruction of irrelevant material and took all practicable steps reasonable in the circumstances to minimise third party impacts. The warrant issuer(s) could authorise interception by a method that might result in collection

---

[32] In other jurisdictions, including the United States and the United Kingdom, the term "bulk collection" is used to describe interception methods that result in substantial acquisition of communications that are irrelevant (or of unknown relevance) to target communications. See, for example, National Research Council *Bulk Collection of Signals Intelligence: Technical Options* (The National Academies Press, Washington DC, 2015); David Anderson QC *Report of the Bulk Powers Review* (HM Stationery Office, August 2016). GCSB prefers not to use the term in relation to its own activities.

[33] Section 17(3)(b) GCSB Act 2003. Following the 2013 amendments the relevant provision was s 15A(2)(b), which required the Minister (and Commissioner where relevant) to be satisfied that "the outcome sought to be achieved under the proposed interception or access justifies the particular interception or access."

of irrelevant information and impacts on third parties, if satisfied that the Act's specific requirements for issuing a warrant were met. The GCSB Act therefore provided scope for collection methods such as "full take".

GCSB policies

63. The Bureau has policies and procedures to guide its staff on how to conduct activities in accordance with the law. Key policies and procedures in place during the period covered by this report addressed:

    63.1. compliance with the prohibition on intercepting the private communications of New Zealanders (and allowable exceptions to it);

    63.2. the prohibition on intercepting privileged communications;

    63.3. minimising the risk of intercepting irrelevant communications;

    63.4. retention and destruction of collected information; and

    63.5. sharing intercepted communications with overseas partner agencies.

Private communications of New Zealanders

64. Intercepting the communications of foreign persons can involve intercepting the communications of New Zealanders, depending on the method used and where the interception occurs. Some collection methods, for example, result in the incidental acquisition of irrelevant communications along with the foreign communications sought. Those may be the private communications of New Zealanders who happen to be in foreign places and/or using foreign communications systems that are subject to interception. Private communications can also be intercepted inadvertently, for example by human error in the collection process (eg a mistake in the entry of a telephone number).

65. Given the constraints on its ability to intercept the private communications of New Zealanders, the Bureau was obliged to assess the risk of doing so when it sought to intercept foreign communications. During the period covered by this report it had several policies and procedures guiding its approach.

New Zealand Signals Intelligence Directive 7: in effect December 2009 - 9 October 2014

66. The New Zealand Signals Intelligence Directive 7: The Collection and Reporting of Foreign Communications (NZSID 7) was revised in December 2009 (replacing a version issued in June 2003) and updated in 2013. It governed the collection, processing, retention and dissemination of foreign signals information by the Bureau for foreign intelligence purposes until superseded by policies reflecting the amended legislation, including the Nationality Policy, which took effect in October 2014.

67. Most of NZSID 7 was declassified and released under the Official Information Act 1982 in November 2014. Much of the Nationality Policy is unclassified.

68. NZSID 7 reflected the agreement between New Zealand and its Five Eyes partner countries to respect each other's limits on interception of their own citizens' private communications. Targeting of communications passing solely between or among New Zealand or Five Eyes country entities was prohibited.[34] For targeting purposes, any dual national of a Five Eyes country and another country would be treated in accordance with their non-foreign status.[35]

69. The directive set out presumptions for dealing with partial information and uncertainty about nationality. These presumptions were starting points for a nationality assessment, but could be rebutted by information to hand. They set out tentative conclusions that could be drawn from known facts about a targeted person. The details remain classified.

70. Where collection proceeded on the presumption that targeted communications were foreign, it had to cease immediately if new information confirmed or suggested they were not foreign. Collection could only resume if the Director was satisfied that the communication was in fact foreign.[36] The 2009 version also noted that any paused or terminated collection could be audited to determine whether interception should have stopped sooner.[37]

71. NZSID 7 established a procedure for determining whether a New Zealand person met the Act's definition of "foreign person" or "foreign organisation", and so could be targeted for interception.[38] It termed such a person an "Agent of a Foreign Power" (AoFP). The identification of a person as an AoFP had to be approved by the Director on legal advice, supported by evidence. Only the communications of an AoFP acting as an agent – not personal communications – could be targeted for collection. AoFP identification could be retrospective: eg if intercepted communications thought to be foreign turned out to belong to a New Zealander, interception would cease but could resume (and communications collected earlier could be retained) if it was established that the person was an AoFP.

72. Under the 2009 version of NZSID 7 metadata was distinguished from the content of communications. Analysis of metadata on the communications of New Zealand persons was not seen as interception of those communications. New Zealand persons or entities were not to be the primary subject of metadata analysis except where a written request was received from a New Zealand government agency.[39]

73. Under the 2013 version of NZSID 7, metadata was identified as a form of communication as defined in the Act. It was not distinguished from content and the 2009 provisions on analysis of metadata were removed.[40] This change followed the 2013 amendment of the statutory definition of "communication," which resolved a legal question about its application to metadata (see paragraph 48 above).

---

34 At [2.5] (2009) and [14] (2013).
35 At [2.2] (2009) and [11] (2013).
36 At [2.22] and [2.24] (2009); at [27]-[28] (2013).
37 At [2.23].
38 At [2.18]-[2.20] (2009) and [23]-[26] (2013).
39 At [2.14]-[2.15].
40 At [21].

Nationality Policy – in effect from 10 October 2014

74. The Bureau reviewed policies and procedures after the GCSB Amendment Act 2013. The Nationality Policy was approved by the Director and took effect from 10 October 2014. Its stated purpose was to outline the way in which the Bureau would ensure compliance with the statutory constraints on intercepting the private communications of New Zealanders. It also covered the prohibition on collecting privileged communications, the duty to minimise impact on third parties, and statutory constraints on retention, destruction and communication of intercepted communications and intelligence. The policy was part of a suite of policies that superseded NZSID 7.

75. The policy provided basic guidance on definitions of citizenship and permanent residency.[41] A person was a permanent resident if he or she held a residence class visa under the Immigration Act 2009. Citizens of the Cook Islands, Niue and Tokelau were New Zealand citizens. Dual nationals were entitled to the protections applying to New Zealand citizens.[42] Australian citizens and permanent residents who came to New Zealand also had to be treated as New Zealand citizens, as they were automatically granted a residence visa on entry.[43]

76. The policy stated that the GCSB would not avoid the legal protections for New Zealanders by asking its intelligence partners for assistance:

> GCSB will never assist a 5-Eyes partner by doing something on the partner's behalf which would be illegal for the partner to do for itself, and will never ask a 5-Eyes partner to do something on its behalf that it would be illegal for GCSB to do for itself.[44]

77. The policy noted the statutory definition of private communication and advised that "a communication is *not* private if it is made in circumstances in which any person should reasonably expect that the communication might be intercepted by a third party who doesn't have consent to do so."[45] It commented that "[i]n the modern digital communications environment, deciding whether or not a communication is private will sometimes be highly complex and rely on a number of factors."[46] Decisions on what was private and what was not were to be made by senior managers, with legal advice as needed.

78. The Nationality Policy maintained the process for identifying a New Zealand person as an 'Agent of a Foreign Power' if he or she met the statutory definition of a foreign person or organisation.[47]

---

41 At [9]-[10].
42 At [12].
43 At [11].
44 At [15].
45 At [25].
46 At [26].
47 At [16]-[18].

79. The policy emphasised the importance of target plans and research plans as records of the reasons for intercepting communications.[48] Target plans and research plans are discussed in my "Report into Government Communications Security Bureau's process for determining its foreign intelligence activity" (June 2017).[49] A target plan sets out reasons for intended foreign intelligence activities, links them to a foreign intelligence purpose; assesses the risk that private New Zealand communications might be encountered during the course of those activities and outlines strategies to manage and respond to the risk.

Customer Requests for Foreign Intelligence – in effect from 15 May 2014

80. A GCSB policy procedure on Customer Requests for Foreign Intelligence, in effect from 15 May 2014, set out how the Bureau would manage customer requests requiring the use of its signals intelligence capabilities. The policy is classified, but the process for dealing with customer requests is also discussed in my earlier report (see paragraph 79 above). No action was to be taken on a customer request without prior risk assessment and a nationality check of any named individual whose private communications were proposed for collection. All requests had to be covered by an appropriate authorisation.

Privileged communications of New Zealanders

81. Until September 2013 the Act did not expressly address the interception of privileged communications. Legal professional privilege was addressed briefly in policy on intelligence reporting. The principal policy on intelligence collection, NZSID 7, never addressed the interception of privileged communications.

82. In the absence of legislative direction, the Bureau asked the then Inspector-General, Hon Paul Neazor QC, for his opinion on the legality of intercepting communications subject to legal professional privilege. He concluded in 2007 that, in some circumstances, GCSB could collect and report legally privileged foreign communications. The Bureau adopted this view.

83. In 2013 the Act was amended to prohibit the issue of any authorisation for the purpose of intercepting the privileged communications of New Zealand citizens or permanent residents.[50] "Privileged communications" meant communications covered by legal, religious or medical privilege.[51] The privileged communications of foreign nationals were not protected.

Nationality Policy – in effect from 10 October 2014

84. The Nationality Policy took effect after the 2013 amendments. It required any collected privileged communications to be treated as irrelevant and destroyed as soon as practicable, as required by section 23 of the Act. If there was any doubt about whether a communication

---

48 At [7].
49 From [105].
50 Section 15C.
51 The categories of privilege are defined under sections 54, 56, 58 and 59 of the Evidence Act 2006.

with a religious, legal or medical adviser was privileged or not, the Chief Legal Adviser was to be consulted.[52]

85. The policy noted that the privileged communications of non-New Zealanders were not protected. As a matter of policy however the Bureau would apply the relevant policies and practices of its Five Eyes partners to the privileged communications of Five Eyes nationals.

Protecting New Zealand and Allied Sensitivities in Intelligence Reporting – in effect from 16 July 2014

86. This policy procedure required a "sensitivity check" on any intelligence reporting containing information relating to legal proceedings in which the New Zealand government was involved, even if the information did not relate to a New Zealand national. The Chief Legal Advisor was to be consulted in any case of hesitation or doubt.[53] Like the Nationality Policy, this policy said the Bureau would apply the relevant policies and procedures of its Five Eyes partners to any intercepted privileged communications of their nationals.[54]

Minimising impact on third parties

87. Section 24 of the Act imposed a duty on the Bureau, in undertaking any interception, to take "all practicable steps that are reasonable in the circumstances" to minimise the likelihood of intercepting communications not relevant to the persons targeted. The primary policies relevant to this duty were those directed at ensuring interception was confined to foreign communications. These are discussed above

88. From 2014 a policy procedure on Target Plans (PP-2016) also stated controls on the use of signals intelligence systems by analysts, according to the purpose of their activity. The key limitation was that a selector (eg a telephone number) could only be specified to a selection system for collection of its associated communications if it was associated with a known foreign intelligence target. A specific selector was not to be targeted for interception for the purpose of target discovery (finding new targets).

89. Structured queries[55] of repositories of intercepted data could be used, however, for both the pursuit of information on targets and target discovery. The risk that a query would extract information about the private communications of New Zealanders, or irrelevant communications of others, was to be managed by structuring the query carefully to maximise the relevance of the results. The policy noted that the extent of the risk would depend on the extent to which the data being queried had been focused by prior selection and filtering. One of the functions of a target plan was to provide guidance on how to structure queries given the particular circumstances of the intelligence target.

---

52 At [27].
53 At [19(vii)].
54 At [7].
55 A structured query is a string of search terms designed to extract relevant information from a database. Queries usually specify multiple terms that are sought, or to be excluded, or both, in an effort to focus the search results on material that is of interest and exclude irrelevant material and false positives.

Retention and destruction of intercepted communications

90. When it intercepted communications the Bureau could legally retain only information relevant to its statutory objectives or functions. All else had to be destroyed. The Act expressed this as a default requirement for destruction of intercepted communications, with limited exceptions. Section 23 required that any record or copy of an intercepted communication had to be destroyed "as soon as practicable after the interception," unless it related to the statutory objectives and functions of the Bureau or met the requirements of section 25. That section specified purposes for which information (or "incidentally obtained intelligence", after the 2013 amendments) could be retained and who the Bureau could share it with. Incidentally obtained intelligence was essentially non-foreign intelligence obtained in the pursuit of foreign intelligence.[56]

91. NZSID 7 required any legitimately intercepted communications to be retained in accordance with the Public Records Act 2005, unless subject to any specific deletion requirements in law.[57] Inadvertently intercepted New Zealand or partner country communications were to be destroyed as soon as practicable upon recognition.[58] The 2009 version made an exception for metadata from such communications, which could be retained "for identification purposes and to assist the understanding of the communications environment."[59] This exception does not appear in the 2013 version, consistent with the clarified legal status of metadata as form of communication under the amended Act (see paragraph 48 above).

92. The Nationality Policy (which superseded NZSID 7 in 2015) cited the statutory obligation to destroy irrelevant material with no foreign intelligence value "as soon as practicable."[60] It detailed the Bureau's practice that material would either be over-written as repositories filled up with newer data, or be deleted automatically ('aged off') after a specific period to be set out in an information management policy. (This policy was applied in draft before it was finalised in 2017). If material was needed for longer than usual (eg for a research project) this would be specified in a Target Plan or Research Plan. Data required for foreign intelligence research would be retained for as long as it remained relevant.

93. A policy specifically on the handling of incidental intelligence (PS-216) was adopted in April 2014. It noted that as incidental intelligence could relate to New Zealanders, any such information would require particular care and sensitivity in handling. It explained that because the definition of "incidentally obtained intelligence" under the Act concerned only material obtained in the course of gathering foreign intelligence, information acquired in the execution of the Bureau's information assurance or cybersecurity activity could not qualify. The policy

---

[56] Section 4 defined "incidentally obtained intelligence as intelligence "(a) that is obtained in the course of gathering intelligence about the capabilities, intentions, or activities of foreign organisations or foreign persons; but (b) that is not intelligence of the kind referred to in paragraph (a)".

[57] At [3.1] (2009) and [29] (2013).

[58] At [3.6] (2009) and [31] (2013).

[59] At [3.7].

[60] At [34].

advised that in assessing whether a communication was foreign intelligence the nationality of the parties was only one relevant aspect. Subject matter and information revealed by metadata were also factors.

Partner collaboration and information sharing

94. Under ministerial authorisation the Bureau could share intelligence with Five Eyes partner agencies.[61] Partner agencies could also share intelligence with the Bureau. The sharing of intelligence could encompass sharing of intercepted communications in unprocessed[62] or processed forms and sharing of analysis and reports.

95. NZSID 7 stated that access to GCSB storage systems containing intercepted communications identifying New Zealand or Five Eyes country entities was ordinarily restricted to Bureau personnel with an established need for access (and to the IGIS). Five Eyes agency personnel with an established need could be granted access with the express prior permission of the GCSB Director.[63] That access, and any collection access, analysis or reporting by GCSB personnel, could be audited for compliance with nationality rules. Any contravention of the rules had to be recorded and brought to the attention of the IGIS, with details of corrective action taken.[64] Where intelligence reporting identified a New Zealand or partner country national, dissemination would be limited to the relevant country's signals intelligence agency unless it authorised otherwise.[65] New Zealand identities would ordinarily be "minimised" (anonymised).[66]

96. The Nationality Policy recognised a risk that foreign intelligence material forwarded by GCSB to its Five Eyes partners might include irrelevant or inadvertently intercepted private communications of New Zealanders. It noted that partner agencies could receive this material on condition they handled it according to the Bureau's rules and policies.

Internal compliance auditing

97. Until late 2013 audit activity within the GCSB was limited to audits of structured queries , including checks of compliance with nationality rules. Following the report of an external review of compliance in March 2013[67] a compliance team was established and a need for compliance auditing identified.

98. Analyst access to information, whether collected by GCSB itself or shared with GCSB by partners, was subject to auditing. Monitoring of compliance with this obligation was

---

61 Authorisations were enabled by sections 8A(c)(ii), 8B(1)(c)(ii) and 8B(2) of the Act.
62 Unprocessed data is often referred to as "raw" data, although this is a more variably applied term.
63 At [2.25] (2009) and [38] (2013).
64 At [4.1]-[4.2] (2009) and [46]-[47] (2013).
65 At [3.15] (2009) and [39] (2013).
66 At [3.9] (2009) and [34] (2013).
67 Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).

introduced in May 2014. A compliance auditor was appointed in late 2014 and several audits of operations were subsequently undertaken. In 2015-16 the compliance audit function became part of a broader compliance adviser role.[68]

GCSB SIGINT processes

99. This section sets out, to the extent possible, the operational processes followed by the Bureau for signals intelligence (SIGINT) collection during the relevant period.

100. Collection originated with requests for foreign intelligence. My June 2017 report on the GCSB's process for determining its foreign intelligence activity set out how the Bureau received and processed requests for foreign intelligence, both before and after the 2013 amendments to its legislation.[69] Broadly, this involved:

- receiving a request from a New Zealand government Minister or agency, or from a government agency in a partner country;
- assessing whether the request was legally valid, whether it would meet a government intelligence requirement and what priority it should be given;
- assessing whether the requested intelligence could be met from existing collection activity or would require new authorisations and/or resources; and
- assessing the risks of proceeding, including the risk of intercepting the private communications of New Zealanders.

101. Where these assessments resulted in a decision to proceed with collection the Bureau would move into operational planning and execution. From late 2013 target plans for specific areas of foreign intelligence activity set out the purposes of collection, risk assessments and risk reduction strategies.

102. In the course of preparing this report I inquired further into the Bureau's SIGINT production chain. I describe it in broad terms in the rest of this section.

Collection requirements

103. From intelligence requirements the Bureau defined collection requirements, then assessed whether they could be met from existing or re-purposed GCSB collection capabilities, by making a request to a partner agency, or from new capabilities that could be established. Collection requirements, which were recorded in a single authoritative database, could identify:

- targets, ie individuals or classes of individuals; entities or classes of entities;

---

[68] More recently the Bureau has re-established and filled a dedicated compliance auditor role.
[69] See parts 3 and 4 of that report.

- communications systems used by targets ; and/or
- generic requirements, such as confidential communications of the target.

104. Collection requirements could be used to define a request to a partner agency to carry out collection using their capabilities.

Authorisation

105. Any new GCSB capability had to fall within an existing authorisation or warrant to be used for interception or access. Where it did not, or where the GCSB wished to remove any ambiguity in its authority to use the capability, a new interception warrant or access authorisation was sought.

Tasking

106. A specialist team issued tasking instructions defining the interception or access that would best meet a collection requirement, to the extent authorised under the relevant warrant or access authorisation. The tasking instructions could define an activity to be undertaken by the GCSB itself (such as satellite interception from Waihopai), or with the assistance of a network operator or service provider compellable under New Zealand law (such as the lawful interception of telephone calls).[70] Tasking instructions were stored in an authoritative database along with a justification for the tasking.

107. The specialist GCSB teams responsible for carrying out collection activities would clarify or confirm tasking instructions if they identified any indicators that a mistake had been made, but primarily relied on the team issuing the instructions to ensure the proposed collection was properly authorised.

108. Partner agencies would follow their own processes for deciding whether to fulfil a GCSB request for collection, including checking that any collection would comply with its own domestic legal obligations.

Collection

109. During the period covered by this report GCSB's collection capabilities included interception of communications relayed by satellite; interception of high frequency radio communications; lawful interception (under the Telecommunications (Interception Capability) Act 2004 and then the Telecommunications (Interception Capability and Security) Act 2013); and the ability to request partner agencies to carry out collection using their capabilities.

110. Depending on the capability used, communications collected by the Bureau would contain varying levels of relevant and irrelevant communications. Interception of traffic on a satellite

[70] Lawful interception was enabled under the Telecommunications (Interception Capability) Act 2004 and subsequently the Telecommunications (Interception Capability and Security) Act 2013.

bearer, for example, would result in collection of a higher proportion of irrelevant communications than interception of a specific telephone line.

111. Wherever possible, GCSB would seek to use specific selectors, such as telephone numbers associated with subjects of intelligence interest, to filter intercepted communications. This process of "selection" enables the identification of the most relevant ("selected") information, which would be retained for longer periods than unselected information.

112. "Full take" was a shorthand phrase used by GCSB to describe the collection and retention of unselected communications data (of certain types) acquired from particular satellite communications links.[71] It was applied only to satellite communications links assessed by GCSB as likely to carry communications of intelligence value. Unselected information collected and retained through "full take" could only be analysed by the application of structured queries.

113. GCSB staff were required to monitor and review collected data at regular intervals to ensure the collection remained compliant and of foreign intelligence value.

Analysis

114. GCSB analysed data for a range of purposes including to discover or identify intelligence targets, develop knowledge or understanding of such targets and understand the configuration and operation of communications networks, or contribute to cryptanalysis. Analysts used structured query tools on both unselected and selected ("filtered") data. These tools commonly (but not always) required entry of a note of the justification for the query.

115. In addition to intelligence gathering, satellite collection would be used for survey purposes, to research the communication systems utilising a particular satellite or identify the satellites servicing an area of interest. Survey data could also be used to evaluate the efficacy of the analysis tools and technologies being used to process collected communications and the accuracy of targeting of satellites and bearers.

Reporting

116. Analyses of collected intelligence prepared by GCSB were called End Product Reports (EPRs). These could be provided to a range of New Zealand government agencies and other 'customers', such as ministers, and to agencies in other countries. Distribution was controlled by the use of classification and other markings and by use of information systems with restricted access. EPRs were typically highly classified and accessible only to people with the necessary security clearances, although less sensitive versions could be produced at lower classifications, for wider distribution, through a process known as 'sanitisation'. Any New Zealand identities would usually be "minimised" (anonymised) in reports.

---

[71] Information on the specific types of data GCSB could intercept and store through "full take" collection is classified.

Data retention

117. Collected foreign intelligence data is retained by the GCSB while analytic work is undertaken. Data that is determined to be of no intelligence value is deleted by a process known as "aging off," by which it is automatically discarded after a fixed period that varies according to the type of data and the space available for its storage.

118. Data retention periods ranged from as little as a few minutes (for unselected information not subject to "full take") to multiple years (for certain types of data specifically known to be relevant). GCSB retained unselected data for a shorter period than selected data. Selected data could be stored for longer than usual if the necessary processing and filtering mechanisms were unknown or under development. This could occur if, for example, an opportunity to collect communications associated with a rarely accessible target arose, but the communications were encrypted.

119. Data used to support reporting is kept as a business record and archived. EPRs are permanently retained. EPRs may also be held permanently by other agencies they have been shared with, whether in New Zealand or other countries. GCSB does not have records of what reports are retained by partner agencies or how often they are viewed.

Data sharing

120. As noted above (under "Partner collaboration and information sharing") partner agency personnel with an established need could be granted access to GCSB intercept storage with the express prior permission of the Director. Collected selected and unselected data could also be forwarded to partner agencies in response to an intelligence request; for analytical support (typically by providing a subset of the data); where GCSB was reliant on partner technology and capabilities to process, make sense of, and store the collected data; or where the intelligence dividend was increased by combining GCSB's collection with that from partners. Forwarding data to a partner would mean GCSB did not retain complete direct control of it and relied on the partner to apply and audit agreed access restrictions and controls on data use.

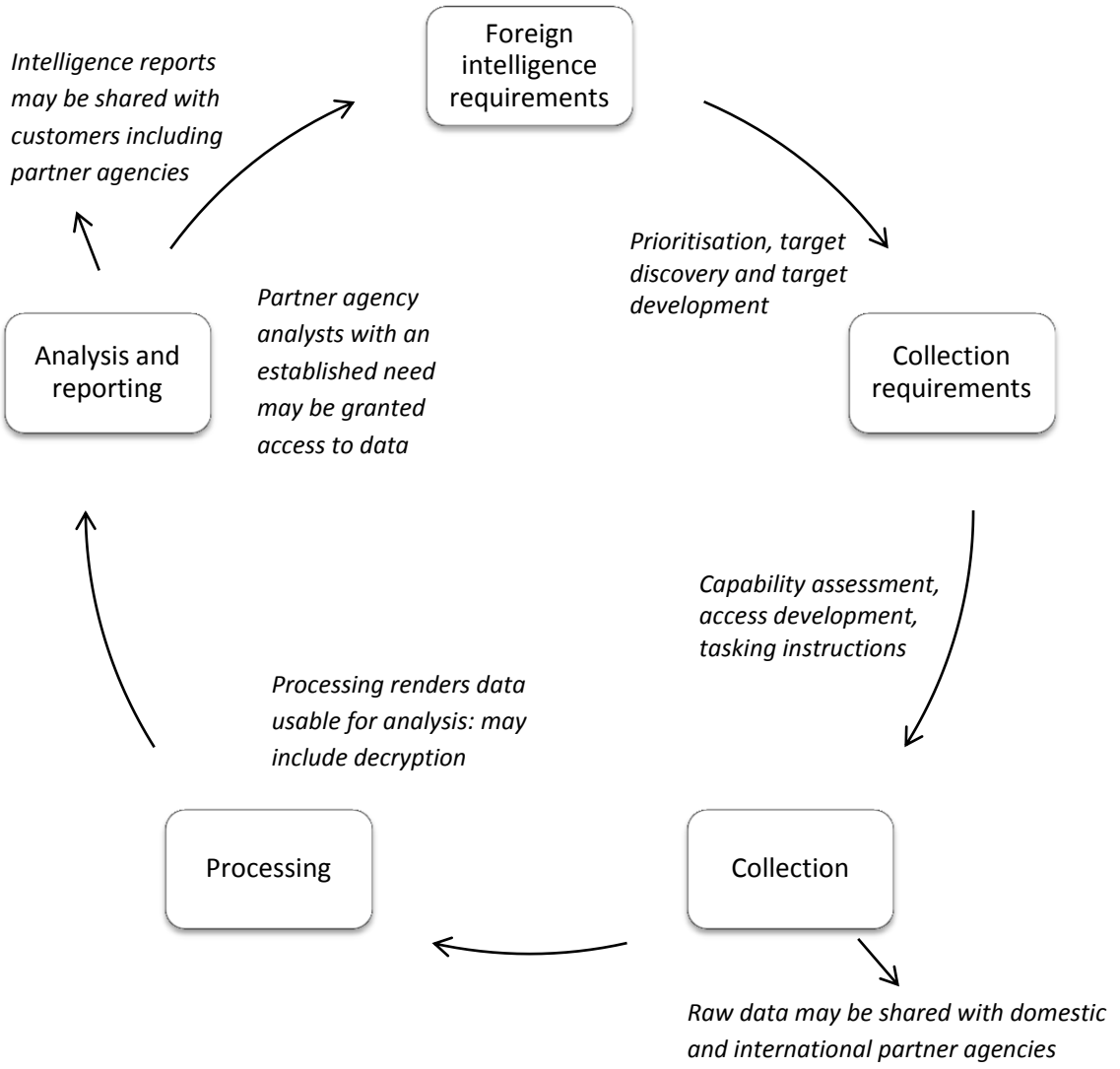
Auditing & Compliance

121. The GCSB required peer review of a sample of structured queries against repositories. Compliance staff would also review a proportion of all logged and auditable queries. Records of structured queries run against GCSB data repositories are retained indefinitely, although not all of the query tools used by GCSB over the relevant period were able to produce a comprehensive list of each query ever entered by an analyst and the results the query delivered.

SIGINT Production Cycle

122. Some signals intelligence collection meets limited short-term purposes, but much is directed at gaining intelligence on matters of enduring interest to decision-makers. Where that is the

case, the end products of collection inform the further development of intelligence requirements and the production chain becomes a cycle:



GCSB ACTIVITY IN RELATION TO THE SOUTH PACIFIC 2009-2015

Context

123. If a country's telecommunications system is connected to rest of the world by satellite, in principle its international communications can be collected by intercepting communications to and from the satellite. Domestic communications can also be intercepted if they pass over a satellite link in a domestic network, eg between remote locations.

124. In the South Pacific a number of the main cities are now connected by undersea cables.[72] Network connections to many outer islands are still provided by satellite, however, and for some of the period covered by this report, some Pacific Islands nations were largely dependent on satellites for the international connections of their telecommunication systems. During the period, cable networks were expanding, as were domestic cellphone networks and cellphone use.[73]

General findings

125. The GCSB undertook signals intelligence-gathering in relation to New Zealand's interests in the South Pacific during 2009-2015. This inquiry did not find any evidence of GCSB activity outside the scope of Government intelligence requirements, as expressed in the (classified) Foreign Intelligence Requirements that were in effect at the time.

126. The GCSB's activity included the collection of telecommunications across satellite links. The collection methods used varied in the extent to which they resulted in acquisition of irrelevant communications along with targeted communications. The GCSB Act anticipated this. The Bureau's methods included "full take" collection, which resulted in acquisition of more irrelevant communications than other methods.

127. There were statutory authorisations in place enabling the GCSB lawfully to collect signals intelligence in relation to New Zealand's interests in the South Pacific during this period. Their details are classified. I did not find evidence to suggest that the GCSB operated beyond the scope of these authorisations, including by use of "full take" collection.

128. Two exceptions were identified by the Bureau's internal compliance process. Both involved inadvertent collection of communications beyond the scope of the relevant authorisations. Both seem to have arisen as a result of misunderstanding of legal parameters rather than institutional disregard for legal controls. One was reported by GCSB to former Inspector-General McGechan, with advice on the corrective action taken. One was not reported to the Inspector-General, but corrective action was taken.

129. I am unable to disclose more specific information on the Bureau's collection capabilities and its activities in relation to New Zealand's interests regarding any particular persons or places in the South Pacific during the relevant period. For reasons of security and international relations it is not possible to disclose publicly full details of what was collected, where, when, and how. I can however address in general terms the possible effects on complainants.

---

[72] A number of submarine cable maps are publicly available online: see, for example, www.submarinecablemap.com.

[73] "South Pacific Islands: Telecoms, Mobile, Broadband - Statistics and Analyses" (Paul Budde Communication Pty Ltd, 2016).

Findings regarding complainants' communications

130. Extensive searches of GCSB holdings in the course of this inquiry did not return any indication that any complainant's communications were deliberately targeted for collection and reporting by the GCSB.

131. Besides deliberate targeting, signals intelligence can result in incidental or inadvertent collection of private communications. This can result from inadvertent targeting (eg through a mistake in entry of a telephone number), or where a person who is not of intelligence interest happens to communicate with a targeted person, or where the communications of a target are collected by means that inherently involve the acquisition of other, irrelevant communications.

132. Searches of GCSB holdings did not return any direct matches relating to complainants that would indicate their communications were collected by the GCSB inadvertently or indirectly, or reported in any way. These searches were appropriately time bound, utilised multiple search terms in relation to each complainant, considered alternative spellings, and where necessary examined fragmentary results.[74] Searches extended to the organisation-wide document management system, email records, SIGINT collection and tasking systems, records of New Zealand persons designated an Agent of a Foreign Power, and repositories containing various streams of End Product Reports.

133. Given the nature of signals intelligence collection processes, however, I cannot entirely rule out the possibility that at some point some complainant communications were incidentally or inadvertently collected in GCSB or partner agency systems. At the most transitory, some communications could have been copied from the systems carrying them, held in a cache of data being machine-scanned for matches with selectors of intelligence interest (eg telephone numbers), then discarded within a few minutes to hours. In short, if any complainant's communications were inadvertently or incidentally collected, there is no evidence that GCSB retains any such data.

134. Likewise it is difficult to determine with certainty whether any complainant's communications were retrieved, even briefly or incidentally, by a structured query of collected data. Although most queries were logged, not all of the query tools used by GCSB over the relevant period were able to produce a comprehensive list of each query ever entered by an analyst and the results the query delivered. If a complainant communicated with an entity of intelligence interest, that communication might have been collected, discovered by a query and examined by GCSB. The absence of any End Product Report or supporting business records referring to any of the complainants, or data associated with them, suggests however that if any such communication existed it was deemed irrelevant for intelligence purposes, discarded, and subsequently deleted through the aging-off process.

---

[74] For instance, if searching GCSB holdings for the term "one", returns would also include any records containing the word "money". The searches conducted examined fragmentary records and discounted these where they were shown to be irrelevant.

135. Any communications collected in even the most transitory way were "intercepted" as defined in the GCSB Act 2003. The Act defined intercept as "…hear, listen to, record, monitor, acquire, or receive a communications, or acquire its substance, meaning or sense."[75] This encompasses communications that were acquired but not read or listened to, or recorded and subsequently deleted, or monitored but not recorded.

136. Given that it is not possible to make a categorical finding on whether or not complainant communications were intercepted in this sense, it is similarly difficult to ascertain whether any records relating to complainants were shared with partners. As outlined in "Data sharing" above, partner agency personnel with an established need could have been authorised to access GCSB data or had it forwarded to them. Given the lack of evidence that any complainant was of any intelligence interest to the GCSB, however, it appears unlikely that any such records existed or were shared.

Findings regarding GCSB compliance procedures and systems

137. The information presented in this report about the GCSB's compliance procedures and systems between 2009-2015 is now largely of historical interest. The procedures and systems relevant to any intelligence activity in relation to New Zealand's interests in the South Pacific were those that applied to the Bureau's foreign intelligence activities in general. These have been scrutinised before, notably in the Kitteridge review.[76]

138. I find that the Bureau had relevant and substantial compliance procedures and systems in place. These covered matters of specific interest to this inquiry and review, such as the application to the people of the Cook Islands, Niue and Tokelau of the protections applicable to New Zealand citizens.

139. Consistent with the findings of the Kitteridge review and other inquiries by my Office, there were gaps and shortcomings in policy and procedure pre-2013, exacerbated by some shortcomings in the GCSB Act 2003. Measures to address these began in 2013 following the legislative amendments and Ms Kitteridge's recommendations. I found nothing to suggest that any intelligence activities in relation to New Zealand's interests in the South Pacific were excluded from the normal application of internal compliance controls and procedures during the period examined.

---

[75] GCSB Act 2013, s 4.

[76] Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).

GLOSSARY

Bulk collection	GCSB does not refer to any of its activities as "bulk collection", but in other jurisdictions, including the United States and the United Kingdom, the term is used to describe interception methods that inherently result in substantial acquisition of communications that are irrelevant (or of unknown relevance), at the time of collection, to target communications. "Bulk collection" is commonly contrasted with "targeted collection", which refers to methods that are more precisely focused at the point of interception, eg on a specific selector or set of selectors. The distinction is not exact, however: bulk collection may be undertaken within parameters designed to focus it to some extent on communications with anticipated intelligence value, while targeted collection generally cannot eliminate all possibility of acquiring irrelevant communications.
Collection	The acquisition of data using signals intelligence capabilities. "Collection" is commonly used in preference to "interception" as a general descriptor of signals intelligence activity as "interception" commonly has a specific legal meaning and/or is used to denote a particular point in the collection process (eg the moment at which a signal is copied from the medium carrying it).
Cryptanalysis	The analysis of encrypted communications to convert them into plain text, when the original encryption algorithm and/or key are unknown.
Filtering	The selection of a subset of data by systematic searching for matches to criteria that identify wanted types of data (for retention), unwanted types of data (for rejection), or both. Filtering typically involves machine (computer) scanning of collected data and may be iterative, so that unwanted data is progressively screened out of the original data set.
Five Eyes	The Five Eyes partnership is an intelligence-sharing arrangement between the United States, the United Kingdom, Canada, Australia and New Zealand.
Focusing	The formulation of collection parameters and/or the application of filters to collected data, with the aim of maximising the relevance of collected and/or stored data to the purpose of collection.
Incidentally obtained intelligence	Under the GCSB Act 2003 "incidentally obtained intelligence" was defined as (in effect) non-foreign intelligence acquired in the course of gathering foreign intelligence (s 4). In some contexts the phrase was also used more informally to refer also to valid foreign intelligence information that was obtained incidentally to targeted information.
Lawful interception	GCSB term for warranted interception carried out with the assistance of telecommunications network operators acting as required under the Telecommunications (Interception Capability and Security) Act 2013 and before that the Telecommunications (Interception Capability) Act 2004.
Processed data	Data that has been subjected to any operation that changes its format, eg from encrypted to unencrypted.

Raw data	Although used variably, “raw data” usually refers to data in the form in which it is collected from the source medium, with no or minimal post-collection processing. The more accurate term is “unprocessed” data.
Repository	A storage location for a data set.
Selector	An identifier of data sought from collection, eg a telephone number associated with a target of intelligence interest.
Selected data	Data filtered by reference to selectors before storage.
Structured query	A set of search terms formulated to extract relevant data from a dataset, entered into a search engine that scans the data. A structured query is comparable to an ‘advanced search’ using an internet search engine, or to the search tools available to users of many specialist databases, where keywords can be combined with search operators (such as the basic Boolean operators ‘and’, ‘or’ and ‘not’) to build strings of search terms that maximise the relevance of the search results. Intelligence agencies use specialised search engines for structured queries rather than publicly available programs.
Survey	The use of signals intelligence capabilities to acquire knowledge about a communications environment (eg the nature, volumes and patterns of communications traffic) rather than being directed at the collection of particular communications of intelligence interest.
Tasking	The definition of parameters for collection, eg a selector, the collection capability to be used, commencement and termination dates and times, the appropriate classification, handling and processing of collected data.
Unselected data	Collected data that has not been filtered by reference to selectors.