Te Pourewa Mātaki
Inspector-General of Intelligence and Security

Review of GCSB and NZSIS activities related to the 2023 General Election

Public Report

Brendan Horsley
Inspector-General of Intelligence & Security
September 2026

CONTENTS

INTRODUCTION

1. I reviewed the activities of the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communications Security Bureau (GCSB or the Bureau) relating to the 2023 New Zealand General Election (the election). [1]

2. Election Day was Saturday 14 October 2023. The three-month regulated period for election advertising began on 14 July. The pre-election period, in which governments generally limit their actions to some extent, conventionally covers those three months.[2]

3. The 2023 election was the third in which the Electoral Commission coordinated the production of protocols for government agencies with election responsibilities, including one specifically on the roles and responsibilities of the GCSB and the NZSIS. This now seems to be an established part of election planning. In my view it has real value.

4. My review looked at the agencies' roles and activities in relation to the election. I was particularly interested in how they dealt with their duty of political neutrality.

5. This unclassified report describes the review outcomes for both agencies, but omits details of operations and methods that cannot be disclosed without prejudice to security.

SUMMARY

6. The agencies have a legitimate role in helping to maintain election integrity. My review found the agencies' activities in relation to the 2023 General Election were lawful and proper. I made no recommendations.

7. The GCSB's activities were within the GCSB's normal cybersecurity mandate. Being confined to cybersecurity matters, they raised few political neutrality issues. The Service's activities invited scrutiny given their role in identifying violent extremist or foreign interference threats to the election.

8. Some of the NZSIS's efforts to discover violent extremist threats to the election involved collecting information about the online activities of individuals and groups with unique or unusual political concerns. I had separately raised with the Service the need for care in noting exactly what rhetoric or behaviour prompted such collection, considering its duty under s 19 ISA to respect freedom of expression. In the course of the review the NZSIS advised me it had added associated prompts to its resources for planning and executing this kind of activity.

9. The Service's efforts to detect any interference in the election by foreign states included looking for possible means of influence, interference actors and vulnerabilities. It also provided

---

1 This was a review under s 158(1)(f) of the Intelligence and Security Act 2017 (ISA).

2 Cabinet Office *Cabinet Manual 2023* at [6.11].

protective security briefings to participants in the electoral process, including some tailored to participants facing specific risks indicated by intelligence.

10. I found no breach by the Service of its duty of political neutrality. Rather, I found evidence of a reasonable alertness within the Service to the risks and sensitivities of intelligence operations involving, or with implications for, political parties and candidates during the election period.

11. My familiar note of caution for the Service is the need for care in recording the reasons for operational and reporting choices that could come under scrutiny in future. This includes a need to keep accurate records of briefings and any other exchanges with political organisations and figures. While the 2023 election passed without incident, the Service could in future be asked to produce records in circumstances where something relevant has occurred.

RELEVANT LAW AND POLICY

12. The agencies' intelligence and protective security functions, and the information assurance and cybersecurity function of the GCSB, give them legitimate roles in helping maintain the integrity of a general election.[3] Elections may be vulnerable to foreign interference. Election campaigns and voting may be targets for terrorism or violent extremism. The information systems on which an election depends may be vulnerable to compromise and exploitation. These risks and threats come within the agencies' mandates and Government intelligence priorities.[4]

13. At the same time, the purpose of the legislation governing the agencies is to protect New Zealand as a free, open and democratic society.[5] It is vital therefore that no action by an intelligence agency, before or during an election, improperly influences or is reasonably suspected of improperly influencing the election.

14. At election time the agencies' statutory duty of political neutrality is especially important. Section 18 of the ISA requires the Director-General of an agency to take "all reasonable steps" to ensure the agency's activities are politically neutral, meaning for example that those activities "are not carried out for the purpose of promoting or harming the interests of any political party or candidate".[6] As departments of state the GCSB and the NZSIS are also required by the Public Service Act 2020 to act in a politically neutral manner.[7]

15. A corollary to the duty of political neutrality is an obligation under the ISA for each agency's Director-General to consult regularly the Leader of the Opposition, "for the purpose of keeping

---

3 Under s 10 of the ISA the agencies collect and analyse intelligence, in accordance with Government priorities, and provide that intelligence to authorised parties. Under s 11 the agencies provide protective security services, advice and assistance to public authorities and others. Under s 12 the GCSB provides information assurance and cybersecurity services to public authorities and others.

4 The National Security Intelligence Priorities, agreed by the Cabinet in June 2023 and published on dpmc.govt.nz, include foreign interference and espionage (including interference with New Zealand's democracy); terrorism and violent extremism; and malicious cyber activity (including threats to critical service providers and infrastructure).

5 ISA, s 3.

6 ISA, s 18(a)(iii).

7 Public Service Act 2020, s 12.

the Leader of the Opposition informed about matters relating to the agency's functions".[8] A former IGIS suggested this served three important purposes:[9]

> - A direct check against any misuse of the considerable powers and resources of the [agencies];
> - Maintenance of the principle that matters of national security should, so far as possible and appropriate, be non-partisan; and
> - Political accountability in security and intelligence matters …"

Election protocols

16. The Electoral Commission (EC), with others including the GCSB and the NZSIS, has for recent general elections produced protocols for government agencies with election responsibilities. For the 2023 election these included protocols on public communications about the election and on managing election disruptions.[10] There was also, for the third time, a protocol specifically on the roles and responsibilities of the GCSB and the NZSIS (the GCSB/NZSIS protocol).[11]

17. The agencies' obligation to remain politically neutral was reflected in the GCSB/NZSIS protocol.[12] It obliged them to engage with Ministers, the Leader of the Opposition, and other relevant people or entities if there was a national security threat to the election.[13]

18. Responding to other national security issues remained "core government business" in the election period and the agencies had to follow the "no surprises" principle and keep Ministers informed.[14] The GCSB/NZSIS protocol noted, however:[15]

> Particular care may be required in relation to exercising the functions or powers of the GCSB or the NZSIS, such as in an investigation, where notifying a Minister may compromise, or be perceived to compromise, the independence of the investigation. Where this may be the case, the Agencies should consider the purpose of the briefing, timing, manner, and scope.

19. Any "specific or credible threat" to the election could be referred to the Officials Committee for Domestic and Security Coordination (ODESC).[16] The ODESC chair would confirm with the agencies involved the briefing arrangements for the Prime Minister, Ministers, and the Leader of the Opposition.[17]

---

8 ISA, s 20

9 Inspector-General of Intelligence and Security *Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011* (25 November 2014) at 128.

10 Electoral Commission *Introduction to inter-agency protocols for New Zealand's 2023 General Election* (August 2023); *Protocol on communications related to the 2023 General Election process* (August 2023); *Protocol on the management of election disruptions* (August 2023).

11 Electoral Commission *Principles and protocols for the GCSB and the NZSIS in relation to the 2023 General Election* (August 2023).

12 At [16].

13 At [35], [42].

14 At [37]-[38].

15 At [39].

16 ODESC is chaired by the Chief Executive of the Department of the Prime Minister and Cabinet, who invites other officials as necessary.

17 At [34].

20. If the agencies identified a threat to one or more registered political parties campaigning in the election the protocol said ODESC "may consider" whether those parties should be offered a threat briefing and/or protective security advice. Impartiality might require any threat briefing and/or advice given to one party to be offered to all other parties.[18]

21. If contacting any person or entity subject to a specific national security threat (eg to enable them to take preventative action or receive help), the agencies were to consider whether their action might "be perceived as political or … become publicly known", in which case the Directors-General were to consult ODESC on how to proceed.[19]

22. Generally the agencies were to avoid making any public comment related to a specific threat to the election. Any public disclosure of an investigation of a national security threat to the election was to be considered by ODESC.[20]

GCSB policy

23. The GCSB had a guidance note for staff on political neutrality.[21] Its statutory references were well out of date, referring to the GCSB Act 2003 (repealed), though the relevant ISA provisions are substantially similar.

24. The note advised GCSB officers to "perform their jobs professionally, without bias towards one political party or another," so the agency "maintains the confidence of its current Minister and of future Ministers".[22] It set out the Director-General's responsibilities for maintaining political neutrality, including consultation with the Leader of the Opposition, and referred staff to their duties of neutrality under the GCSB Code of Conduct.[23]

25. Other GCSB policy required approval from the Director-General for any intelligence activity against an MP (or a former MP, if the activity relates to their time in office). As it happened the GCSB's activities in relation to the 2023 election were limited to cybersecurity support. The normal suite of policies applying to the delivery of such support applied.

NZSIS policy

26. The NZSIS also addressed its political neutrality obligation in policy. This noted (among other things) that the Director-General may brief the Prime Minister or Leader of the Opposition, as either office holders, or as leaders of their respective parties, being clear about which role applied. It directed staff to be alert to the political sensitivities of any proposed activity, ensuring it could be clearly connected to the agency's statutory obligations, functions and Government intelligence priorities.

---

18 At [44].
19 At [45].
20 At [47].
21 GCSB "Political Neutrality Guidance for GCSB Staff" (undated).
22 At [1].
23 At [5]-[6]. The code of conduct said GCSB employees are required to "Observe political neutrality in the performance of their duties" (GCSB Code of Conduct (23 April 2012, updated October 2019), at 4.

27. They were to ask:[24]

    a. could this activity be viewed as interfering in the democratic process?

    b. could this activity be seen to favour (or undermine) one political party (or group) over another?

    c. could this activity undermine the government's (or any future government's) confidence in the NZSIS's ability to provide impartial advice?

    d. is this advice/assessment inappropriately influenced by political concerns?

    e. is this activity in the spirit of the public service's commitment to political neutrality?

    f. could this undermine public trust in the NZSIS?

28. The policy noted that Ministers are obliged to respect the political neutrality of the public service and not ask officials to act in a way that would conflict with it. And:

> … neither the Director-General nor the wider NZSIS is subject to the direction of the Minister with respect to the commencing, concluding or conduct of any operations or investigations. Such matters may, of course, be discussed with the Minister, but only factors that are relevant to national security may be taken into account when taking operational decisions.

29. An NZSIS policy on "sensitive category individuals" required approval from the Director-General for any intelligence activities involving Members of Parliament (MPs), or former MPs if the activity relates to their time in office. The Service was also obliged by a Memorandum of Understanding (MOU) to brief the Speaker of the House of Representatives on any investigation of an MP or any NZSIS operations at Parliament or an MP's constituency office.[25] The briefing requirement did not extend to any intelligence activities against "a constituent or other person with whom a particular MP is associated or in contact".[26]

30. NZSIS intelligence gathering and protective security activities in relation to an election were otherwise subject to the suite of policies governing those activities generally.

THE GCSB'S ROLE IN RELATION TO THE ELECTION

31. Under the GCSB/NZSIS protocol the GCSB's key responsibilities were to:[27]

- provide cyber security and information assurance services and advice to authorised individuals and entities, including MPs and Ministers;

- develop and provide intelligence and cyber assessments on the intentions, activities, and capabilities of threat actors; and

---

[24] "NZSIS Policy – Political Neutrality" (26 July 2023). The Policy sets out the NZSIS legislative obligations to act in a politically neutral way.

[25] "Memorandum of Understanding between the New Zealand Security Intelligence Service and The Minister Responsible for the [NZSIS] and the Speaker of the House of Representatives of New Zealand, relating to NZSIS Intelligence Activity" (4 June 2019) at [5.5]. There is an exception for urgency (at [5.10]).

[26] At [5.15].

[27] *Principles and protocols for the GCSB and the NZSIS in relation to the 2023 General Election*, above n 11, at [19].

- take any lawful "necessary or desirable action" to protect important communications and information infrastructures, including the Electoral Commission's core systems.

32. The GCSB supported the administration of the election through its National Cyber Security Centre (NCSC) and Computer Emergency Response Team (CERT).[28]

33. The NCSC provided enhanced cyber security to the EC and its key suppliers over the election period, in case of any attempted interference with election-related systems. As with other NCSC cybersecurity support this was by consent of the EC.[29]

34. The NCSC began testing the proposed scope of its election-related activity with the EC before the election period. It produced a pre-election threat assessment, noting (among other things) that New Zealand's paper-based voting process worked against any malicious cyber actors who might seek to interfere with the integrity of the final election results. The most significant risk was disruption from interference with organisations (eg contractors) supporting the EC.

35. After finalising its cybersecurity risk assessment of the EC's system and supply chain the NCSC planned how it would check for any compromise on the EC system. It ran a cyber incident exercise with the EC and key suppliers and gave them advice on cybersecurity threats and preparedness. With CERT it prepared advice for election candidates.

36. On one occasion, the NCSC triaged possible malicious activity, and on "at least two" occasions it alerted the EC or a key supplier to a system vulnerability. It gave advice to an independent organisation whose online pre-election event was disrupted (though was unable to determine whether that was due to malicious cyber activity).

37. Overall, the NCSC saw no significant cyber threat to the election, and on election day NCSC found no indication of malicious activity on EC networks.

38. During the election period the GCSB monitored for websites or pages masquerading as official election-related material and CERT was prepared to issue take-down requests if any were found. CERT (and after CERT's integration, the NCSC) also looked for malicious social media posts relating to the election, eg any with cyber threat indicators such as hidden or malicious links. In the event there were no election-related takedown requests.

39. Over the election period the GCSB/NCSC briefed multiple entities on election cybersecurity, including candidates, senior officials committees and an operational support group for the EC. The Director-General briefed political party presidents (with the NZSIS) and updated Five Eyes partner agency heads at normally scheduled meetings. The NCSC also updated New Zealand and Five Eyes partner officials at routine meetings. The GCSB included information on its support to the election process in its regular written update to its Minister. For Election Day, the NCSC defined arrangements for escalating its reporting of any significant cyber incident, according to severity.

---

[28] CERT was integrated with the GCSB on 31 August 2023. It supported the EC both before and after integration.

[29] Deed Relating to Consent to and Provision of Assistance between GCSB and the EC (2020); letter of agreement (4 September 2023).

40. After the election the NCSC, CERT, the EC and other officials reviewed lessons learned, noting some room for improvement on communications between officials during the election period, but no major concerns.

THE NZSIS'S ROLE IN RELATION TO THE ELECTION

41. Under the GCSB/NZSIS protocol the NZSIS's key roles in relation to the election were to:[30]

    a. collect, analyse and assess intelligence about national security threats against New Zealand and New Zealanders;

    b. … be the government's lead operational agency into whether foreign interference against the election occurred and/or if state-sponsored disinformation relating to the election occurred;

    c. co-lead with New Zealand Police on domestic violent extremism … [as intelligence lead, with Police as response lead].

    d. provide intelligence, assessments, and advice to decision-makers;

    e. … provide protective security services, advice, and assistance to public authorities, including Members of Parliament and Ministers; and

    f. administer the security clearance system ....

42. These responsibilities extended past the election, for example the Service provided protective security briefings to new MPs and conducted security clearance assessments for new Parliamentary staff.

43. My review examined NZSIS efforts to discover any violent extremist threats to the election and any attempts at foreign interference in the election. I also reviewed two investigations of individuals suspected of foreign interference.

Efforts to detect violent extremist threats and foreign interference

44. Throughout the election period the Service assessed acts of election-related violent extremism as unlikely. In fact none occurred, though the Service saw an expected increase in violent rhetoric. After the formation of the new Government the NZSIS looked for any violent extremist reaction to ministerial appointments or other decisions or announcements.

45. Some of the agency's efforts to discover violent extremist threats to the election involved collecting information about the online activities of individuals and groups with unique or unusual political concerns. I had separately raised with the Service the need for care in noting exactly what rhetoric or behaviour prompted such collection, considering its duty under s 19 ISA to respect freedom of expression. In the course of this review the NZSIS advised me that it had added prompts for this in its resources for planning and executing this kind of activity.

46. The Service's efforts to detect any interference in the election by foreign states included looking for possible means of influence, interference actors and vulnerabilities. It also provided

[30] *Principles and protocols for the GCSB and the NZSIS in relation to the 2023 General Election*, above n 11, at [22].

protective security briefings to participants in the electoral process, including some tailored to participants facing specific risks indicated by intelligence.

47. I found the relevant intelligence collection to be lawful and proper. Seeking the information came within the Service's intelligence function and its role under the GCSB/NZSIS protocol as the lead operational agency on foreign interference. Its judgement on where to look for possible indications of attempted foreign influence or interference was reasonable. None of its activities conflicted with its obligations in the MOU with the Speaker, its policy requirements relating to MPs as "sensitive category individuals", or its duty of political neutrality. Some collected data that was meant to be destroyed after analysis remained in an NZSIS system and the agency corrected this when it was noted by my review.

48. The Service's protective security briefings preceding the election were appropriate, as were its decisions on when and to whom to report election-related intelligence.

Investigations of individuals for potential interference

49. The two investigations reviewed both looked at individuals suspected of seeking to exert influence in the interests of a foreign power. One was not solely election-related, but had a clear connection due to an association between the target and a political figure. The NZSIS's inquiries resulted in it providing a protective security briefing to that person, and I was satisfied the agency did nothing contrary to its duty of political neutrality. Its reporting of the relevant intelligence was carefully controlled.

50. The other investigation sought to determine whether a person officially connected to a foreign power was covertly supporting an election candidate. In my view the investigation was well justified and the intelligence collection activities were lawful and proper. In contrast to the other investigation the Service did not brief the relevant party on the intelligence it collected, apparently because of its high classification. I did not see any plausible issue of bias or partisanship in this. Rather, it seemed a question of effectiveness, which is not my remit.

Briefings to political leaders over the election period

51. As noted earlier, the agencies remain accountable to the Government over the election period and must continue to brief ministers in accordance with the "no surprises" principle. They must also consult regularly with the Leader of the Opposition.

52. The Service had records of briefings delivered before and after the election but I was not satisfied from my review that it could account fully and accurately for all briefings to political leaders. The occurrence of some briefings was recorded without any record of the substance. In one case the agency had talking points but nothing to indicate what was actually delivered.

53. It is obvious, I think, that exactly what an intelligence agency passes on to political leaders in relation to election and its aftermath should be very clear in its records. This office has had to inquire, in the past, into a matter involving a briefing to the Leader of the Opposition.[31] Who is

[31] *Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011,* above n 9.

told what and when at the political level can become highly sensitive and the Service should have precise and reliable records of its exchanges with political figures.

CONCLUSION

54. I concluded the GCSB and NZSIS's activities in relation to the 2023 General Election were lawful and proper.

55. The GCSB's election related activities (through the NCSC and CERT) were within the GCSB's normal cybersecurity mandate and its role under the election protocol.

56. Being focused on cybersecurity, the Bureau's election-related activity presented no major challenges in maintaining political neutrality. The NCSC had well-established thresholds for action and reporting of cyber threats. There had to be a direct link to national security before it might take any action, such as reporting or disrupting malicious cyber activity, that might influence (or be seen as influencing) the course of the election. The agency also took a neutral, technical stance on election-related public discourse, eg assessing websites or social media content as malicious according to the presence of standard cyber threat indicators, not content.

57. I noted the Bureau's written guidance on political neutrality was long out of date, referring to pre-ISA legislation. I did not think there was a pressing need to update this (the content was not otherwise defective) but drew it to the agency's attention.

58. It is very helpful, I think, both for oversight and for the agencies themselves, to have the election protocols setting out departmental responsibilities and the roles of the intelligence agencies in particular. This now seems to be an established part of election planning. It seems to me the agencies' continued involvement in producing the protocols is well worth the time involved.

59. In the Service, I found evidence of a reasonable level of alertness to the risks and sensitivities of intelligence operations involving, or with implications, for political parties and candidates during the election period. The agency's political neutrality policy prompts its officers to ask the right questions. Records of the operations conducted over the 2023 election period show signs of those questions being asked. Sensitive decisions were appropriately taken at a high level.

60. I found nothing of concern in the Service's sharing and reporting of election-related intelligence. Sharing was focused in the pre-election period on providing protective security advice, including to political parties and figures possibly subject to attempts at foreign interference. Post-election reporting carefully balanced the need to supply specific information on threats with the need for caution in identifying their targets, with the most specific reporting given high classification and limited distribution.

61. My note of caution for the Service is the need for care in recording the reasons for operational and reporting choices that could potentially come under scrutiny, and for accurate records of briefings and any other exchanges with political organisations and figures. While the 2023 election passed without incident, the Service could in future be asked to produce records in circumstances where something relevant has occurred.