Principles and Protocols for managing NZSIS and GCSB engagement on foreign state threats and cyber-security threats to the 2017 election

August 2017

Purpose and summary

1. There are heightened sensitivities during an election period, which require particular care and restraint. To that end, this document sets out principles and protocols to manage engagement by the New Zealand Security Intelligence Service (NZSIS) and Government Communications Security Bureau (GCSB), in the event that a foreign-state actor attempts to interfere in New Zealand's 2017 general election, or there is a cyber-security threat that threatens to undermine it.

2. This document outlines the obligations that both the NZSIS and the GCSB are subject to, but will apply with particular force around an election. It stresses the neutrality of actors such as the Chief Electoral Officer. It notes the independence and responsibilities of the Director of Security and the Director of the GCSB. Without detracting from those obligations, it describes the role of ODESC and the National Security System, which in particular provide coordination and a sounding board.

Context

3. In light of recent attempts to intervene in elections in Western liberal democratic nations, it is important to consider how the NZSIS, GCSB, and New Zealand's wider National Security System might respond in the event there is a foreign-state or cyber-security threat to New Zealand's 2017 general election. This could include a threat to the electoral process itself or as a wider influence campaign.

4. The integrity of New Zealand's electoral process is at the heart of our democratic society – elections must be free and fair. This includes providing the conditions for citizens to exercise their rights to freedom of political opinion and expression and ensuring that citizens have trust and confidence in both the integrity and reliability of the electoral process. Any responses to a threat to the electoral process must be managed to avoid any perception that those actions in any way undermine the free and fair conduct of the democratic process.

5. During an election, increased public attention can be expected on the way public servants and State agencies carry out their functions. The work of government must always be carried out impartially, and in a manner that cannot be perceived as reflecting party interests. The general principles guiding conduct by all agencies and public servants apply in all circumstances but come into sharper relief during an election period. There is, therefore, a

risk that activities will be perceived to have a political character in a way those actions would not at any other time. Given the intrusive powers of the intelligence and security agencies, this will particularly be the case where any action or decision relates to the conduct of the election or activities undertaken in an electoral context.

Political neutrality and protection of right to lawful advocacy, protest and dissent

6. In responding to any threat, the NZSIS and GCSB must have regard to their full range of obligations, including the obligation of political neutrality as set out in section 4AA(1) of the New Zealand Security Intelligence Service Act 1969 (NZSIS Act) and section 8D(3) of the Government Communications Security Bureau Act 2003 (GCSB Act). Neither NZSIS nor GCSB may take any action for the purpose of furthering or harming the interests of any political party in New Zealand. Political neutrality therefore is not a principle for engagement but a *requirement* that underpins all of the NZSIS' and GCSB's activities. The obligation preserves the integrity of the public sector and an agency's ability to work with any future government. Specific obligations of political neutrality will continue to apply to the agencies under the Intelligence and Security Act 2017 (in force from 28 September 2017).

7. How those obligations work in practice for the NZSIS and GCSB is also informed by the Inspector-General of Intelligence and Security's (IGIS) comments in the *Report into the release of information by the New Zealand Security Intelligence Service on July and August 2011.* In that report, the IGIS stated that "the essence of the obligation of political neutrality is that the NZSIS should not promote or damage the interests of particular political groups, use its intrusive powers to target lawful political activity, or act in a politically partisan way." This was reiterated in the *Report into Government Communications Security Bureau's process for determining its foreign intelligence activity* (released in June 2017).

8. The obligation to be politically neutral requires the NZSIS and GCSB to be independent and impartial in responding to any threat, including in responding to any requests from the responsible Minister. It may, on occasion, require positive and independent action by Directors to uphold or restore political neutrality.

9. The NZSIS and GCSB must have regard to the "No Surprises" principle to ensure that Ministers are kept informed of matters within their portfolio (guidance is set out in the Solicitor-General's letter of 13 September 2016, to chief executives). Particular care may be required in relation to functions or powers, such as 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 NZSIS and GCSB should consider the purpose of the briefing, timing, manner and scope as set out in the "No Surprises" guidance.

10. In addition to these specific obligations of political neutrality, the NZSIS Act recognises the right of persons to engage in lawful advocacy, protest and dissent and provides that the exercise of that right does not, of itself, justify the NZSIS instituting surveillance of any person or entity in New Zealand. This protection is broadened under the Intelligence and Security Act to recognition of the right to freedom of expression (including the right to advocate, protest or dissent), and will apply to both agencies when the new Act comes fully into force.

11. The Directors of the NZSIS and GCSB are concerned to ensure that there is no real or perceived breach of these obligations in the event that there is a foreign-state or cyber-security threat to the 2017 general election. Placing safeguards around those agencies' engagement in responding to any threat will also enable them to perform their functions effectively.

The roles of NZSIS and GCSB

12. The specific objectives and functions of NZSIS and GCSB are currently set out in their individual legislation (the Intelligence and Security Act 2017 will not come into force before the 2017 general election). The Directors are responsible for the performance of the functions, duties, and powers in their respective agencies. The NZSIS and/or GCSB will have a role in responding to a threat to New Zealand's election where that threat is, or may be from a foreign-state actor, or is directly relevant to the performance of one or more of the agency's functions.

13. The agencies' core role is to contribute to the protection and advancement of New Zealand's national security and international and economic well-being. NZSIS and GCSB both have intelligence collection and protective security functions, and support New Zealand's national security through a range of activities including intelligence collection and analysis; providing advice to ministers, public authorities and others; cyber incident detection and response; and supporting the wider National Security System.

14. New Zealand takes an 'all hazards' approach to national security, underpinned by seven key objectives. One of these objectives is "[m]aintaining democratic institutions and national values – preventing activities aimed at undermining or overturning government institutions, principles and values that underpin New Zealand society."

15. In the event a foreign-state or cyber-security threat to New Zealand's election materialises, NZSIS and GCSB will have an important role to play in understanding and responding to that threat.

16. The specific objectives and functions of NZSIS and GCSB are currently set out in their individual legislation. The NZSIS and/or GCSB will have a role in responding to a threat to New Zealand's election where that threat is, or is likely to be, from a foreign-state actor or is directly relevant to the performance of one or more of the agency's functions.

17. There may be threats to the electoral process that will not require NZIC involvement. For instance, the response to the criminal implications of any threat activity will be led by New Zealand Police. The response to some cyber incidents may be led by CERT NZ. There is also very little that a state can do to combat misinformation or 'fake news', particularly given it can be difficult to distinguish from legitimate political discourse. Identifying and responding to fake news is most likely to sit with the media, platforms such as Facebook, and the individual reader. Free and open political communication is a key mitigation.

GCSB

18. The GCSB's functions are outlined in section 8 of the GCSB Act: information assurance and cybersecurity (section 8A), intelligence gathering and analysis (section 8B), and co-operation with other entities to facilitate their functions (section 8C).

19. In the context of a threat to the election, the GCSB is most likely to be asked to provide advice and assistance with information assurance and cyber security, including cyber-incident response. Under section 8A(a), GCSB can "co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister, on any matters relating to the protection, security, and integrity of –

    i. communications, including those that are processed, stored, or communicated in or through information infrastructures; and

    ii. information infrastructures of importance to the Government of New Zealand".

20. The GCSB provides cyber security guidance and baseline technical security standards through the Information Security Manual, which is an integral component of the Protective Security Requirements. It also operates through outreach to government agencies and other organisations of national significance.

21. Cyber security response activities will either be carried out with the consent of the affected person or organisation, or in accordance with a warrant. In providing cyber security services, GCSB only accesses the data and systems necessary to provide those services. GCSB also applies technical measures to protect any personal and other confidential material obtained as a result of those activities.

NZSIS

22. NZSIS's functions are set out in section 4 of the NZSIS Act. They relate to the collection and provision of advice on matters relevant to security. 'Security' is defined in the NZSIS Act. Three limbs of that definition may be relevant in the context of a threat to New Zealand's election.

23. The first is the subversion element of part (a): "the protection of New Zealand from acts of espionage, sabotage, and subversion, whether or not they are intended to be committed within New Zealand". Subversion is defined in the NZSIS Act as "attempting, inciting, counseling, advocating or encouraging -

    i. the overthrow by force of the Government of New Zealand; or

    ii. the undermining by unlawful means of the authority of the State in New Zealand".

24. The second is part (b), namely the "identification of foreign capabilities, intentions, or activities within or relating to New Zealand that impact on New Zealand's international well-being or economic well-being."

25. The third is part (c): “the protection of New Zealand from activities within or relating to New Zealand that:

    i. are influenced by any foreign organisation or foreign person; and

    ii. are clandestine or deceptive, or threaten the safety of any person; and

    iii. impact adversely on New Zealand’s international well-being or economic well-being.”

When will these principles and protocols apply?

26. The principles and protocols in this document have been developed to guide the NZSIS and GCSB in managing threats to the 2017 election. They emphasise the particular need for care and restraint in view of the heightened sensitivities during the election period (the three month period before the election, election day itself, and the period up until the formation of the government).

27. The principles and protocols do not supplant existing agency guidelines and standard operating procedures for day-to-day work, including routine interactions with Ministers and/or political parties and for managing the agencies’ political neutrality obligations. Dealing with sensitive information is also business-as-usual activity for the agencies. For example, the GCSB has processes in place to protect commercially-sensitive and personal information when providing cyber-incident response services.

28. Checks, balances and oversight are built into the intelligence and security agencies’ powers, functions and internal processes. If, for instance, NZSIS needs to conduct a warranted investigation in relation to a threat to the election, the case for issue must be made to the Minister and, where that investigation includes a New Zealand person, the Commissioner of Security Warrants. The NZSIS will need to demonstrate that any action is both necessary and proportionate. Where the investigation includes a New Zealand person, a warrant may be issued with conditions.

29. Further constraints include that warrants may be issued subject to any terms and conditions considered advisable or desirable in the public interest, a means by which particular sensitivities associated with an investigation may be managed. The NZSIS Act also requires the Minister and where relevant, the Commissioner of Security Warrants, to consider whether to include conditions in a warrant to minimise any risk that the warrant may affect third parties if they consider such a risk to be significant.

30. The Intelligence and Security Act re-enacts the necessity and proportionality criteria and also requires the GCSB and the NZSIS to demonstrate that the purpose of the warrant cannot be reasonably achieved by a less intrusive means. The warrant criteria will also require that the authorising officer/s be satisfied that there are satisfactory arrangements in place to ensure that all reasonably practicable steps will be taken to minimise the impact of the proposed activity on any members of the public.

31. Depending on the circumstances, a cyber-based threat to New Zealand’s election may lead to the activation of New Zealand’s Cyber Security Emergency Response Plan.

32. ODESC will be responsible for providing all-of-government coordination, strategic advice on priorities and risk mitigation, and supporting Ministerial decision-making.

Principles to guide engagement by the NZSIS and GCSB

33. These principles underpin NZSIS and GCSB activity at all times. They are particularly important in the context of a threat to New Zealand's election in view of the fact that there are heightened sensitivities during election periods. While NZSIS and GCSB need to maintain operational responsiveness and effectiveness, there is a need for particular care during this period.

Free and fair elections

34. Free and fair elections are central to democracy, with voting rights being protected by the New Zealand Bill of Rights Act 1990, as is the complementary right to freedom of expression. In making any decisions about responding to a threat to New Zealand's general election, the need for a democratic election to be free and fair must be borne in mind. This includes both the need to protect the election and electoral process from any unlawful interference, to maintain its integrity, and the ability and willingness of persons to exercise their right to freedom of expression (including lawful advocacy, dissent and protest).

Respect for lawful political activity

35. Individuals have the right to lawful advocacy, protest and dissent. As recognised in the NZSIS Act and the Intelligence and Security Act, exercise of these rights does not in itself justify NZSIS investigative activity. The IGIS has repeatedly stated that intrusive powers cannot be used to target lawful political activity. The NZSIS and GCSB will not target lawful political activity.

Accountability

36. The NZSIS and GCSB will carry out all activities in a manner that facilitates effective oversight, including through keeping appropriate records of their activities, any key meetings and decision-making processes. Where a threat to the election triggers the activation of the National Security System, the NZIC will alert the IGIS to any response activities underway in accordance with these principles and protocols.

Confidentiality

37. The NZSIS and GCSB will, to the extent necessary, keep confidential the fact that an investigation or incident response is underway. Confidentiality obligations will be context-specific but include maintaining the secrecy of NZSIS and GCSB activities where appropriate, including protecting sources and partner intelligence. This will need to be balanced against the need for transparency.

38. The NZSIS and GCSB will keep ODESC and officials supporting ODESC fully informed.

Good faith

39. In some instances, a decision will need to be made without complete information (for example without a high-confidence assessment of attribution) and/or in balancing a range of

sensitivities. In making these kinds of decisions and in carrying out all activities, the NZSIS and GCSB will be guided by a principle of good faith – making the best possible judgment based on the available information.

Timeliness

40. National security threats often move quickly and the system therefore must also be agile in its response. The NZSIS, GCSB, and NAB should use best endeavors to provide timely analysis, assessment and/or advice.

Transparency

41. The NZSIS and GCSB will work closely with ODESC and officials supporting ODESC, in the event the National Security System is engaged.

42. The NZSIS and GCSB will carry out all activities concerning threats or apparent threats to the electoral process in as transparent a manner as possible, including providing appropriate reporting to relevant government agencies not part of ODESC, Ministers, and the Leader of the Opposition. Transparent action and decision-making will support the principles of impartiality and accountability. However, a balance will also need to be struck between transparency, the need for confidentiality, and how proximate the activity is to constituting a threat to the election. Operating in a transparent fashion does not mean the agencies are required to provide public comment or disclose information where it would undermine the investigation or wider security interests.

Protocols to guide engagement with Ministers, other agencies, political parties and/or candidates

Engagement of the National Security System

43. A foreign-state or cyber-security threat to New Zealand's election, even if only suspected, is a matter of grave and significant importance. In this context, it is important that any response is swift and effective, and properly informed, including by covert intelligence.

44. If there is a genuine possibility of foreign state interference, or it is reasonably suspected, the National Security System will be engaged. Early activation of the National Security System is important, given the sensitivities associated with the election and/or electoral process, which are likely to make a threat both more significant and complex.

45. Activation of the National Security System may involve watch groups (senior officials' meetings, to ensure high-level coordination between agencies and coordinate assessments and advice to ODESC), and ODESC meetings (provide strategic direction, support to the lead agency, and links to the political level, including the National Security Committee).

46. In response mode, the composition of ODESC will depend on the characteristics and consequences of the event. There is no fixed attendance. An ODESC meeting on this topic is likely to be comprised of some or all of the Chief Executives of the Department of the Prime Minister and Cabinet, Ministry of Justice, and Ministry of Foreign Affairs and Trade; the Directors of the GCSB and NZSIS; the State Services Commissioner; and the Commissioner of

Police. Advice may also be sought from the Solicitor-General where required. Similar agencies would be involved in a watch group.

Role of the Electoral Commission and the Chief Electoral Officer

47. The Electoral Commission is an independent Crown entity, with a particular duty of statutory independence conferred by section 7 of the Electoral Act 1993. This duty recognises the Commission's unique role in the New Zealand system and its objectives of administering the electoral system impartially, efficiently and effectively. Any engagement with the Electoral Commission therefore must be carefully managed to avoid any real or perceived risk to the independence of the electoral system. However, the Electoral Commission may seek assistance from any state sector agency to facilitate the effective administration of an election.

48. Given its duty of independence and specific role in the system, the Electoral Commission is unlikely to be directly involved in any response to a threat to the 2017 election unless a specific threat has been identified related to the Electoral Commission's systems or the processes for which the Commission is responsible. The current Chief Electoral Officer may be briefed on relevant threat intelligence. Neither the Chief Electoral Officer nor the Electoral Commission should be asked to provide comment on any policy or incident response measures proposed by ODESC, unless the proposed response includes decisions that will need to be taken by the Electoral Commission. The Electoral Commission cannot be directed by Ministers or ODESC but may receive information, suggestions and offers of assistance.

49. Where necessary, ODESC agencies may also seek advice from the Electoral Commission about appropriate ways to engage with political parties and candidates.

Engagement with Ministers

50. A government has a three-year mandate to govern. Nonetheless, governments, by convention, restrict their actions to some extent in the period immediately before a general election. Responding to events of national security concern remains core government business.

51. In the event a genuine threat to the 2017 general election is identified, the Chair of ODESC should brief the Prime Minister, and other ODESC agencies relevant portfolio ministers, in the usual fashion, in accordance with the principles identified above and the "No Surprises" principle. The timing and nature of that briefing should be well coordinated through the National Security System.

52. The Minister in Charge of the NZSIS and Responsible for the GCSB may also be briefed on a threat in the course of applying for a warrant under either the NZSIS Act or GCSB Act.

Involvement of other government agencies

53. Threats to the electoral system engage a range of interests beyond security. A number of other agencies not represented on ODESC will have an interest in any action taken around such threats. ODESC should ensure agencies with an interest or with responsibilities that overlap are involved as appropriate.

Engagement with the Leader of the Opposition

54. Both the NZSIS and GCSB have a statutory requirement to consult regularly with the Leader of the Opposition for the purpose of keeping him or her informed about security matters and matters related to the GCSB's functions. The IGIS has described consultation with the Leader of the Opposition as an important safeguard, aimed at "building a relationship of trust and confidence with the Leader and his or her party as a 'government in waiting'".

55. The Leader of the Opposition will be provided with these principles and protocols. If a genuine threat to the 2017 general election is identified, the Leader of the Opposition should be briefed on the assessment and any supporting intelligence. Because of the sensitivity of the issue, the Leader of the Opposition should also be informed of any proposed policy or incident response measures.

Engagement with other political parties

56. If a threat is identified that will affect one or more of the other registered political parties campaigning in the general election, ODESC may consider whether those parties should be offered a threat briefing, along with advice on potential mitigations. The need to act impartially may also require that any threat briefing and/or advice on mitigations provided to one political party be offered to all other political parties.

57. If threat information needs to be disseminated outside of the usual channels, ODESC may decide how best to disseminate that information, based on advice from the Director of Security or the Director of the GCSB.

Public communications

58. NZIC agencies will generally avoid making any media comment related to a threat to the 2017 election unless public communications has been agreed as a response to that threat. In that case, any public communications will be developed independently by the National Security Communications Directorate of the Department of the Prime Minister and Cabinet.

59. Any talking points will be provided in advance to the Chief Electoral Officer, Prime Minister, and Leader of the Opposition. These will be provided for their information on a 'no surprises' basis.