DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

Principles and protocols for GCSB and NZSIS in managing foreign interference and cyber security threats to the 2020 General Election

Principles and protocols for GCSB and NZSIS in managing foreign interference and cyber security threats to the 2020 General Election

Purpose and summary

1. Foreign interference and cyber security threats pose a risk to the 2020 General Election and the referendums (the General Election process).[1] The New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB) have a role to effectively address such threats during the heightened sensitivities of an election period. This document sets out principles and protocols to support GCSB and NZSIS (collectively known as the 'agencies') in performing their mandated functions during the election period in relation to managing foreign interference[2] and cyber security[3] threats to the General Election process.
2. While drawing on obligations that both GCSB and NZSIS are subject to at all times, including those under the Intelligence and Security Act 2017 (the Act), this protocol only applies during the election period to the agencies' activities relating to foreign interference and cyber security threats to the 2020 General Election process.[4]
3. For the avoidance of doubt, the protocol does not apply to the agencies' business as usual activities during the election period (or outside of the election period), nor does it replace existing GCSB or NZSIS policies, guidelines or standard operating procedures for business as usual activities. This protocol does not govern the provision of generic protective security and cyber security briefings or work to counter foreign interference that does not have a direct link to the General Election process, routine interactions with Ministers and/or political parties, or managing the agencies' political neutrality obligations. Dealing with sensitive information is also business as usual activity for the agencies.[5]
4. The protocol acknowledges the independence and responsibilities of the Director-General of Security and the Director-General of the GCSB. It considers the threshold at which GCSB

[1] As per the other election protocols, the 'General Election process' refers to the pre-planning and delivery of the 2020 parliamentary election, as well as the two referendums being held with the 2020 election.

[2] Foreign interference refers to an act by a foreign state, or its proxy, that is intended to influence, disrupt or subvert a New Zealand national interest by covert, deceptive or threatening means.

[3] A cyber security incident is defined as an occurrence or activity that appears to have degraded the confidentiality, integrity or availability of an information infrastructure.

[4] For the purpose of the protocols, the 'General Election process' refers to the pre-planning and delivery of the 2020 national election, as well as the two referendums being held with the 2020 General Election.

[5] For example, GCSB has processes in place to protect commercially-sensitive and personal information when providing cyber-incident response services.

and NZSIS would engage the Chief Electoral Officer and the National Security System[6], of which the agencies are a part. Further information about this engagement is set out in the *Protocol on the management and response to election disruption* and supplemented by internal planning documents maintained by GCSB and NZSIS.

Context

National Security System and the protection of democratic society

5. 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."[7] This approach is complemented by the Government's National Security and Intelligence Priorities, which focus the agencies' efforts on the areas of greatest national security interest to the Government.
6. 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 New Zealanders 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.
7. General principles guiding the conduct of all government agencies and public servants apply in all circumstances but come into sharper relief during an election period. Setting out in advance the principles and processes that will guide any response to a foreign interference or cyber security threat to the electoral process will help protect GCSB and NZSIS from any perception that their actions in any way reflect political party interests or undermine the free and fair conduct of the democratic process.
8. In light of recent attempts by foreign states to intervene in elections in liberal Western democratic nations, it is important to consider how GCSB, NZSIS, and New Zealand's wider National Security System might respond in the event there is a foreign interference or cyber security threat to New Zealand's 2020 General Election. This could include a threat to the electoral process itself, a wider influence campaign or a 'hack and leak' scenario.
9. A foreign interference or cyber security threat to New Zealand's 2020 General 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 classified intelligence.

---

[6] New Zealand's National Security System (NSS) has two primary functions – (a) strategic governance and (b) coordinated crisis response and recovery. The governance function focuses on the architecture that provides for the proactive and coordinated management of risks that threaten national security. The crisis response and recovery function focuses on coordinating efforts to mitigate the immediate impacts of an event or emergency that meet certain criteria, and to ensure that longer-term recovery needs are managed appropriately.

[7] National Security System Handbook 2016, p.8.

Links to other protocols

10. This protocol applies specifically to foreign interference or cyber security threats to the General Election process. Other disruptions to the election are covered in the *Protocol on the management and response to election disruptions*, which:

    a. outlines the approach being taken by the Electoral Commission and other government agencies to mitigate and manage hazards and threats which may disrupt the General Election process; and

    b. describes how the National Security System will support and enable all-of-government coordination if the integrity of the electoral process is threatened or disrupted.

11. The *Protocol on communications related to the 2020 General Election process* outlines the roles of agencies in managing misleading or inaccurate information about the General Election and referendums. Agencies will work together to ensure any issues of this nature are directed to the most appropriate agency based on their existing functions and powers.

The roles of GCSB and NZSIS

12. The specific objectives and functions of GCSB and NZSIS are set out in the Intelligence and Security Act 2017 (the Act). The Directors-General of GCSB and NZSIS are responsible for the performance of the functions, duties, and powers of their respective agencies.

13. The agencies' core role is to contribute to the protection and advancement of New Zealand's national security, international relations, and well-being. GCSB and NZSIS 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 in accordance with the Government's priorities, providing that intelligence to Ministers, the Chief Executive of DPMC and other authorised persons, and providing protective security services, advice and assistance to public authorities and other authorised persons.

14. The Act requires that the agencies must be politically neutral, that the Directors-General must regularly consult the Leader of the Opposition, and that the exercise of a person's freedom of expression does not of itself justify an intelligence and security agency taking any action in respect of that person. Additional duties under the Act that are of particular relevance to the General Election process are that GCSB and NZSIS must act:

    a. in accordance with New Zealand law and all human rights obligations recognised by New Zealand law;

    b. independently and impartially in the performance of their operational functions;

    c. with integrity and professionalism; and

    d. in a manner that facilitates democratic oversight.

15. In the event a foreign interference or cyber security threat to the General Election process materialises, GCSB and NZSIS will have an important role to play in understanding and responding to that threat.

GCSB

16. GCSB's key roles in relation to managing foreign interference and cyber security threats to the General Election process are to:

    a. provide cyber security and information assurance services and advice to authorised individuals and entities. This includes Members of Parliament, Ministers and other entities involved in the conduct of the General Election process;

    b. develop and provide intelligence (primarily foreign intelligence) and cyber assessments on the intentions, activities and capabilities of threat actors, including in relation to the General Election process; and

    c. do everything, within the bounds of the law, that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information infrastructures. This includes the Electoral Commission's core systems.

17. GCSB provides cyber security guidance and baseline technical security standards through the Information Security Manual[8], which is an integral component of the Protective Security Requirements.[9] GCSB also operates through outreach to government agencies and other organisations of national significance.

18. Cyber security response activities will either be carried out with the consent of the affected person or organisation, or in accordance with a warrant under the Act. 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

19. NZSIS's key roles in relation to managing foreign interference threats to the General Election process are to:

    a. collect, analyse and assess intelligence about foreign interference activities in New Zealand. The particular focus is on understanding the activities and motivations of foreign state actors operating in, or seeking to influence, New Zealand institutions, processes and individuals;

    b. provide intelligence to decision-makers;

    c. provide protective security services, advice and assistance to a wide range of individuals and entities, including Members of Parliament and Ministers; and

    d. administer the security clearance system which helps to protect the New Zealand Government against the risks of insider threat and espionage.

[8] https://nzism.gcsb.govt.nz/

[9] https://protectivesecurity.govt.nz/

Checks, balances and oversight

20. Checks, balances and oversight are built into the agencies' powers, functions and internal processes. The Act enables GCSB and NZSIS to undertake certain activities if authorised by a warrant. Warrants are authorised by the Minister Responsible for the GCSB and the NZSIS and, if the proposed warranted activity is for the purpose of doing anything directly in relation to a New Zealander, a Commissioner of Intelligence Warrants.

21. The Inspector-General of Intelligence and Security provides independent oversight of GCSB and NZSIS to ensure the agencies conduct their activities legally and with propriety.

Principles

22. In addition to duties under the Intelligence and Security Act [paragraph 14 refers], the *Introduction to inter-agency protocols for New Zealand's 2020 General Election* contains a number of principles that apply to all State sector agencies. These are:

    a. the conduct of elections is a fundamental expression of New Zealanders' democratic values;

    b. New Zealanders are aware of and are encouraged to participate in the 2020 General Election and referendums;

    c. the Electoral Commission is responsible for the conduct of free and fair elections;

    d. Government agencies support the conduct of the elections; and

    e. responses to disruptions throughout the election period are effective, coordinated and proportionate.

23. These are supplemented by the following principles which acknowledge the attributes of foreign interference and cyber security threats and the need for GCSB and NZSIS to maintain operational responsiveness and effectiveness. GCSB and NZSIS will:

    a. use best endeavours to provide timely analysis, assessment and/or advice;

    b. make judgments based on the available information, guided by the professional discipline of intelligence assessment and the principle of good faith;

    c. to the extent necessary and appropriate, keep investigations or incident responses confidential. While confidentiality obligations will be context-specific, they may include maintaining the secrecy of GCSB and NZSIS activities where necessary (for example, to protect national security), including protecting classified information such as sources and partner intelligence; and

    d. keep key stakeholders and relevant agencies informed of activities concerning threats or apparent threats to the electoral process to the greatest extent possible and appropriate.

24. It will be necessary to strike a balance between the need for confidentiality and keeping key stakeholders and relevant agencies informed. Keeping key stakeholders and relevant agencies informed does not mean that GCSB and NZSIS are required to provide public comment or disclose information where it would undermine an investigation or wider security interests.

Thresholds and escalation process

25. It may be necessary to escalate matters to the National Security System to enable all-of-government coordination, the provision of strategic advice on priorities and risk mitigation, and to support Ministerial decision-making at appropriate and relevant levels. In the first instance, and as explained in the *Protocol on the management and response to election disruption*, the expectation for the General Election process is that all agencies will continue to use existing 'business as usual' processes and procedures when planning for, and responding to, disruptive events.

26. In practice, this means that for managing foreign interference and cyber security threats to the General Election process, GCSB and NZSIS will draw on existing information-sharing and escalation processes as much as possible. If another agency (for example New Zealand Police, CERT NZ, Netsafe, or the Electoral Commission) becomes aware of a suspected foreign interference or cyber security threat to the election they will notify GCSB and/or NZSIS as relevant.

27. If GCSB and/or NZSIS become aware of, or reasonably suspect, specific foreign interference activity or a cyber security incident threatening the General Election process, or there are credible or reasonable allegations of either that may significantly impact public confidence in the electoral process, they should seek to escalate any concerns through the standard National Security System escalation process as consistent with the thresholds set out in the National Security System Handbook (see page 24 of the Handbook).

28. The Directors-General may also seek to escalate matters to the National Security System should they wish to keep relevant agencies appraised of a developing situation or to seek the collective advice of relevant agencies.

29. Once made aware of any matters of potential national security concern, the National Security System will follow its standard consideration process at the appropriate decision-making levels as described both in the National Security Handbook and as outlined as relevant to the elections in the *Protocol on the management and response to election disruptions.* While not constraining the discretion of the Chair of the Officials' Committee for Domestic and External Security Coordination (ODESC), it is expected that a core group of chief executives would likely be involved in any ODESC meeting convened in relation to a cyber security or foreign interference threat to the 2020 General Election. The group will likely comprise the Chief Executives from the Department of the Prime Minister and Cabinet, GCSB, NZSIS, the Ministry of Justice, the Ministry of Foreign Affairs and Trade, the State Services Commission, and the Crown Law Office. Other agencies, with particular reference to the Electoral Commission, would be invited to attend as appropriate.

30. If a Watch Group or an ODESC meeting takes place regarding a suspected foreign interference or cyber security threat to the 2020 General Election, the Chair will confirm with agencies the briefing arrangements for the Prime Minister, Ministers, and the Leader of the Opposition. This discussion will be held in the context of the agencies' obligations under the Intelligence and Security Act 2017.

Engagement with affected persons or entities, Ministers, the Leader of the Opposition, and political parties

31. GCSB and or NZSIS may need to engage with a range of persons or entities regarding a foreign interference or cyber threat to the General Election process. These engagements fall into two broad categories:

    - Ministers and the Leader of the Opposition; and
    - affected or potentially affected persons or entities.

32. It is possible that the agencies may need to engage with a person in more than one capacity. For example, a Minister or the Leader of the Opposition may need to be informed in that capacity, but may also be considered to be potentially affected by a foreign interference or cyber threat. Should such a case arise, it will be important that any engagement with people or entities clearly identifies in what capacity they are being engaged.

Engagement with Ministers and the Leader of the Opposition

Ministers

33. Responding to events of national security concern remains core government business in the pre-election period.

34. GCSB and NZSIS must consider the "no surprises" principle as set out in the Cabinet Manual.[10] This states that, as a general rule, officials should inform Ministers promptly of matters of significance within their portfolio responsibilities, particularly where these matters may be controversial or may become the subject of public debate. Particular care may be required in relation to exercising the functions or powers of the GCSB or NZSIS, 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, GCSB and NZSIS should consider the purpose of the briefing, timing, manner and scope.

35. In the event of a specific or credible threat to the General Election process, the National Security System will be activated. Engagement with the Prime Minister and other Ministers should follow the process in paragraph 30 and be in accordance with the principles outlined in this protocol.

36. In addition, GCSB and/or NZSIS may need to engage the Minister Responsible for the GCSB and the NZSIS in order to apply for a warrant under the Intelligence and Security Act 2017 (and this process may include consultation with the Minister of Foreign Affairs). Acknowledging the operational independence of the agencies, this process remains unchanged. The Directors-General would keep ODESC (in the form described in paragraph 29) appraised of the progress of any relevant national security investigation.

[10] Cabinet Manual 2017, paragraph 3.22(a), 3.22(b).

The Leader of the Opposition

37. GCSB and NZSIS have a statutory requirement to consult regularly with the Leader of the Opposition for the purpose of keeping him or her informed about matters relating to the agencies' functions. In the event of a specific threat or credible allegations of a threat, the National Security System will be activated, and it is expected that the Directors-General will carry out their statutory function to consult with the Leader of the Opposition in accordance with the process outlined in paragraph 30 and the principles outlined in this protocol.

Engagement with affected or potentially affected persons or entities

Political parties

38. Members of Parliament have received preparatory protective security and cyber security briefings from GCSB and NZSIS. These briefings are intended to equip those receiving them to protect themselves from potential foreign interference or cyber security threats ahead of the 2020 General Election.

39. If a threat is identified in the election period that will affect one or more of the other registered political parties campaigning in the 2020 General Election, ODESC may consider whether those parties should be offered a threat briefing, along with advice on potential specific 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.

Affected persons or entities

40. GCSB and NZSIS have standard practices for engaging a person or entity subject to a specific known cyber security or foreign interference threat. Engagement may allow the person or entity to take preventative action and the agencies to provide assistance where appropriate. Where such activity has the potential to be perceived as political or to become publicly known, the Directors-General will consult with ODESC on the content of any notification to affected persons or entities.

Other entities

41. If threat information needs to be disseminated outside of the usual channels, ODESC will consider how best to disseminate that information, based on advice from the Directors-General.

Public communications

42. GCSB and NZSIS will generally avoid making any public comment related to a specific threat to the General Election process. Public communications should follow the processes outlined in the *Protocol on communications related to the 2020 General Election process* and the *Protocol on the management and response to election disruptions.* Decisions regarding any public disclosure of an investigation of foreign interference or cyber security threat would be subject to ODESC consideration.

Brook Barrington

Chair of ODESC
Chief Executive, Department of the Prime Minister and Cabinet

Date: 03 July 2020

Rebecca Kitteridge

Director-General of Security

Date: 02 July 2020

Andrew Hampton

Director-General of the GCSB

Date: 01 July 2020