



Te Kāwanatanga o Aotearoa
New Zealand Government



**ELECTORAL
COMMISSION**
TE KAITIAKI TAKE KŌWHIRI

Principles and protocols for the GCSB and the NZSIS in relation to the 2023 General Election

August 2023

Principles and protocols for the GCSB and the NZSIS in relation to the 2023 General Election

Purpose and summary

1. New Zealand's holding of a General Election in 2023 falls during a period in which, internationally, there have been notable attempts by malicious cyber actors, foreign states, and violent extremists to disrupt democratic processes. It is therefore important to consider how New Zealand would manage potential threats to the 2023 General Election.
2. The New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB) (collectively known as the 'Agencies') have a role in addressing national security threats to New Zealand's sovereignty, including democratic systems and processes such as elections. An election period is a time where both threats and sensitivities may be heightened.
3. This document sets out principles and protocols to support the Agencies in performing their mandated functions, particularly in relation to managing foreign interference¹ and cyber security threats² to the 2023 General Election under the [Intelligence and Security Act 2017](#) (hereafter the ISA). This document outlines some of the Agencies' lead and supporting roles and provides transparency in how they will support other government agencies responsible for the delivery and conduct of the election. This protocol only applies to the 2023 General Election.
4. 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.
5. This protocol does not govern the provision of generic protective security and cyber security briefings or work to counter national security threats to New Zealand that do not have a direct link to the General Election, routine interactions with Ministers and/or political parties, or

¹ Foreign interference refers to an act by a foreign state, or often acting through a proxy, which is intended to influence, disrupt or subvert New Zealand's national interests by covert, deceptive, corruptive or threatening coercive means.

² Cyber security events include:

- cyber security incidents: occurrences or activities that appears to have degraded the confidentiality, integrity or availability of an information infrastructure, and which are business as usual activities for the GCSB, and
- cyber security emergencies, which are incidents or combinations of incidents that cause significant and sustained disruption to digital systems critical to health and safety, New Zealand's economic well-being, international reputation or democratic institutions, and require a significant and coordinated response through activation of the ODESC system.

For more information see the Cyber Security Emergency Response Plan on the DPMC website: https://www.dPMC.govt.nz/sites/default/files/2021-08/New_Zealands_Cyber_Security_Emergency_Response_Plan.pdf

UNCLASSIFIED

managing the Agencies' political neutrality obligations. Dealing with sensitive information is also business as usual activity for the agencies.³

6. The protocol acknowledges the operational independence and responsibilities of the Director-General of Security and the Director-General of the GCSB. It considers the threshold at which the agencies would engage the Chief Electoral Officer and New Zealand's strategic crisis management system (hereafter referred to as the ODESC-system) of which the agencies are a part. Further information about this engagement is set out in the *Protocol on the management of election disruptions* and supplemented by internal planning documents maintained by the agencies.

³ For example, GCSB has processes in place to protect commercially sensitive and personal information when providing cyber-incident response services.



Context

The ODESC System and the protection of democratic society

7. The ODESC system⁴ has been used as the governance mechanism for overseeing strategic crisis response for a wide range of threat and hazard-caused crises since 2001. It continues to perform this function today, 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.”⁵
8. This approach is complemented by the Government’s National Security Intelligence Priorities.⁶ The Priorities define key areas of interest where intelligence should support government to make informed decisions about national security. They support intelligence and assessment agencies⁷ to prioritise effort and add value to decision-making on national security matters.
9. 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 they have trust and confidence in both the integrity and reliability of the electoral process.
10. 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 the management of a national security threat to the electoral process will help protect the GCSB and the 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.
11. A national security threat to New Zealand’s 2023 General Election, such as a foreign interference or cyber security threat, even if only suspected, would be a matter of grave and significant importance. This could include a threat to the electoral process itself, a wider influence campaign, or a data breach or disclosure of private information targeting candidates and/or political parties. In this context, any response must be swift and effective, and properly informed, including by classified intelligence. It is therefore important to consider how the Agencies, New Zealand’s wider national security community, and the ODESC system might respond and support the Electoral Commission in the event that such a threat materialises during the election period.

⁴ The ODESC (Officials’ Committee for Domestic and External Security Coordination) system was previously known as the National Security System.

⁵ National Security System Handbook 2016, p.8, available at: <https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf>

⁶ The National Security Intelligence Priorities can be viewed here: <https://www.dpmc.govt.nz/our-programmes/national-security/national-security-intelligence-priorities>

⁷ Many government agencies contribute intelligence and assessment on national security, including: New Zealand Customs Service, New Zealand Police, New Zealand Defence Force, Ministry of Foreign Affairs and Trade, the Department of the Prime Minister and Cabinet, GCSB and NZSIS, Ministry of Business Innovation and Employment and Ministry for Primary Industries.

Links to other protocols

12. This protocol applies specifically to the role of the NZSIS and the GCSB in relation to the 2023 General Election. The aim of the *Protocol on the management of election disruptions* is to:
 - a. outline 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. describe how the ODESC System will support and enable all-of-government coordination if the integrity of the electoral process is threatened or disrupted.
13. The *Protocol on communications related to the 2023 General Election process* outlines the roles of various government agencies in managing certain misleading or inaccurate information about the General Election, including misinformation and disinformation during the election period. All relevant 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 the GCSB and the NZSIS

14. The specific objectives and functions of the GCSB and the NZSIS are set out in the ISA. The Directors-General of the GCSB and the NZSIS are responsible for the performance of the functions, duties, and powers of their respective agencies.
15. The Agencies' core role is to contribute to the protection and advancement of New Zealand's national security, international relations, and well-being. The Agencies support New Zealand's national security through a range of activities including intelligence collection and analysis, providing intelligence assessments to Ministers, the Chief Executive of the Department of the Prime Minister and Cabinet (DPMC) and other authorised persons, and providing protective security services, advice and assistance to public authorities and other authorised persons.
16. The ISA requires that actions of the Agencies are politically neutral. There is also a requirement for the Directors-General to regularly consult the Leader of the Opposition to keep them informed about matters relating to the Agencies' functions.
17. Duties under the ISA that are of particular relevance to the General Election process are that the Agencies must act:
 - a. in accordance with New Zealand law and all human rights obligations recognised by New Zealand law, including the protection of freedom of expression;
 - 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.
18. In the event a foreign interference or cyber security threat to the General Election materialises, the GCSB and the NZSIS will have a particularly important role to play in understanding and responding to that threat.

The GCSB

19. The GCSB's key roles in relation to the General Election 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;
- 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; and
- c. in accordance with the law, take any necessary or desirable action 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.

20. The GCSB provides cyber security guidance and baseline technical security standards through the Information Security Manual⁸, which is an integral component of the Protective Security Requirements.⁹ The GCSB also operates through outreach to government agencies and other organisations of national significance.

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

The NZSIS

22. The NZSIS's key roles in relation to the General Election are to:

- a. collect, analyse and assess intelligence about national security threats against New Zealand and New Zealanders;
- b. with respect to foreign interference, be the government's lead operational agency and source of assessment into whether foreign interference against the election occurred and/or if state-sponsored disinformation¹⁰ relating to the election occurred;
- c. co-lead with New Zealand Police on domestic violent extremism¹¹. New Zealand Police are the national Response Lead and NZSIS (including CTAG) is the Intelligence Lead. While mis and disinformation have the potential to inspire people to violence, they are not the main focus but rather form part of the environment of the NZSIS's investigations into violent extremism;

⁸ See: <https://nzism.gcsb.govt.nz/>

⁹ See: <https://protectivesecurity.govt.nz/>

¹⁰ Disinformation is false or modified information knowingly and deliberately shared to cause harm or achieve a broader aim. Misinformation is information that is false or misleading, though not created or shared with the direct intention of causing harm.

¹¹ Violent extremism is the justification of violence to achieve a change in government, religion or society.

UNCLASSIFIED

- d. provide intelligence, assessments, and advice to decision-makers;
- e. as Government Protective Security Lead, manage the Protective Security Requirements framework¹² which outlines New Zealand's best practice in relation to protective security, and provide protective security services, advice, and assistance to public authorities, including Members of Parliament and Ministers; and
- f. administer the security clearance system which helps to protect the New Zealand Government against national security risks.

Checks, balances and oversight

23. Checks, balances, and oversight are built into the Agencies' powers, functions and internal processes. The ISA enables the GCSB and the NZSIS to undertake otherwise unlawful activities if authorised by a warrant. Warrants are authorised by the Minister Responsible for the GCSB and the NZSIS and, if the subject of warranted activity is a New Zealand citizen or New Zealand permanent resident, a Commissioner of Intelligence Warrants.
24. The Inspector-General of Intelligence and Security provides independent oversight of the GCSB and the NZSIS to ensure the Agencies conduct their activities legally and with propriety.

¹² <https://protectivesecurity.govt.nz/>



Principles

25. In addition to duties under the ISA [[paragraph 14 refers](#)], the *Introduction to inter-agency protocols for New Zealand's 2023 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 2023 General Election;
 - 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.
26. These are supplemented by the following principles which acknowledge the attributes of national security threats and the need for the agencies to maintain operational responsiveness and effectiveness. The GCSB and the NZSIS will:
- a. use best endeavours to provide timely analysis, assessment and/or advice;
 - b. make judgements 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 the GCSB and the NZSIS's activities and equities 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 national security threats or apparent threats to the electoral process to the greatest extent possible and appropriate.
27. 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 the agencies are required to provide public comment or disclose information where it would undermine an investigation or wider security interests, or inadvertently affect the election itself.

Thresholds and escalation process

28. It may be necessary to escalate matters to the ODESC 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 of election disruptions*, the expectation for the General Election is that all agencies will continue to use existing 'business as usual' processes and procedures when planning for, and responding to, disruptive events.
29. In practice, this means that for managing national security threats to the electoral process, the agencies 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 national security threat to the election they will notify the GCSB and/or the NZSIS.

30. If the Agencies become aware of, or reasonably suspect, a specific and credible national security threat to the electoral process or its outcome, they should seek to escalate any concerns through the standard ODESC system escalation process in accordance with the thresholds set out in the National Security System Handbook (see page 24 of the [Handbook](#)).¹³
31. The Directors-General may also seek to escalate matters to the ODESC system should they wish to keep relevant agencies apprised of a developing situation or to seek the collective advice of relevant agencies.
32. Once made aware of any matters of potential national security concern, senior officials in the ODESC system will follow the 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 of election disruptions*.
33. While not constraining the Chair of ODESC's discretion, it is expected that a core group of chief executives would likely be involved in any ODESC meeting convened in relation to a foreign interference or cyber security threat to the 2023 General Election. The group will likely comprise the Chief Executives from DPMC, the GCSB, the NZSIS, the Ministry of Justice, the Ministry of Foreign Affairs and Trade, the Public Service Commission, and the Crown Law Office. Other agencies, with particular reference to the Electoral Commission, would be invited to attend as appropriate.
34. If a Watch Group or an ODESC meeting takes place regarding a specific and credible national security threat to the 2023 General Election, the Chair will confirm with attending agencies the briefing arrangements for the Prime Minister, Ministers, and the Leader of the Opposition, as appropriate. This discussion will be held in the context of the Agencies' obligations under the ISA – which are included in the following sections.

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

35. The Agencies may need to engage with a range of persons or entities regarding a national security threat to the General Election. These engagements fall into two broad categories:
 - Ministers and the Leader of the Opposition; and
 - affected or potentially affected persons or entities.
36. 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 national security 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.

¹³ Note, the Handbook has not yet been updated to reflect the change in terminology from the use of 'National Security System' to 'ODESC system'. However, ODESC continues to perform a crisis management function across all hazards/all risks, and the handbook content regarding crisis management is otherwise up to date.

Engagement with Ministers and the Leader of the Opposition

Ministers

37. Responding to events of national security concern remains core government business in the election period.
38. The Agencies must continue to consider the “no surprises” principle as set out in the Cabinet Manual, throughout the election period.¹⁴ This principle 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.
39. 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.
40. In the event of a specific or credible threat to the General Election, the ODESC system will be activated. Engagement with the Prime Minister and other Ministers should follow the process in paragraph 34 and align with the principles outlined in this protocol.
41. In addition, the Agencies may need to engage the Minister Responsible for the GCSB and the NZSIS in order to apply for a warrant under the ISA (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 32) apprised of the progress of any relevant national security investigation.

The Leader of the Opposition

42. The GCSB and the NZSIS have a statutory requirement to consult regularly with the Leader of the Opposition for the purpose of keeping them informed about matters relating to the agencies’ functions. In the event of a specific threat or credible allegations of a threat, the ODESC 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 34 and the principles outlined in this protocol.

Engagement with affected or potentially affected persons or entities

Political parties

43. Ahead of the 2023 General Election, the Agencies are providing protective and cyber security guidance to all candidates, which will be accessible via the Electoral Commission’s portal. The Agencies have also invited the Presidents/Secretaries of parties currently in Parliament to a protective and cyber security briefing. These briefings will be delivered with the New Zealand Police, who will provide physical security advice.
44. If a threat is identified in the election period that will affect one or more registered political parties campaigning in the 2023 General Election, ODESC may consider whether those parties should be offered a threat briefing and/or protective security advice, along with advice on potential specific mitigations. The need to act impartially may also require that any threat

¹⁴ [Cabinet Manual 2023, paragraph 3.26\(a\)](#).

briefing and/or advice on mitigations provided to one political party be offered to all other political parties.

Affected persons or entities

45. The Agencies have standard practices for engaging a person or entity subject to a specific national security 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

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

Public communications

47. The Agencies will generally avoid making any public comment related to a specific threat to the General Election. Public communications should follow the processes outlined in the *Protocol on communications related to the 2023 General Election process* and the *Protocol on the management of election disruptions*. Decisions regarding any public disclosure of an investigation of a national security threat to the 2023 General Election would be subject to ODESC consideration.



Rebecca Kitteridge

**Te Tumu Whakarae mō Te
Tari o te Pirimia me te
Komiti Matua**

**Chief Executive, Department
of the Prime Minister and
Cabinet |**

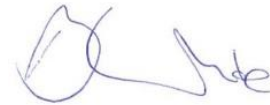
Chair of ODESC



Andrew Hampton

**Te Tumu Whakarae mō Te
Pā Whakamarumarū**

Director-General of Security



Bridget White

**Te Tumu Whakarae mō Te
Tira Tiaki**

**Acting Director-General of
the GCSB**