Te Tira Tiaki
Government Communications Security Bureau

Te Pā Whakamarumaru
New Zealand Security Intelligence Service

Proactive release of material

The following document has been prepared for proactive release by the GCSB and NZSIS on behalf of Hon Chris Penk, Minister Responsible for the GCSB and NZSIS.

Date	Title
June 2026	Briefing to the Incoming Minister

Some parts of the information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh withholding it.

Key to redaction codes

Section	Explanation
6(a)	To avoid prejudice to the security or defence of New Zealand or the international relations of the Government of New Zealand
9(2)(ba)(i)	To protect information subject to an obligation of confidence, where revealing it would prejudice the supply and it is in the public interest that it continue to be supplied
9(2)(f)(iv)	To maintain the constitutional conventions for the time being to protect the confidentiality of advice tendered by Ministers of the Crown and officials.
9(2)(g)(i)	To maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown.

MIN-2026-021

Te Tira Tiaki
Government Communications Security Bureau

Te Pā Whakamarumaru
New Zealand Security Intelligence Service

Briefing to the Incoming Minister 2026

Table of Contents

Introduction

1. Congratulations on your appointment as the Minister Responsible for the Government Communications Security Bureau (GCSB), and Minister Responsible for the New Zealand Security Intelligence Service (NZSIS). We look forward to working with you to achieve the Government's objectives.

2. As set out in the Intelligence and Security Act 2017, our work contributes to:

   - The protection of New Zealand's national security;
   - The international relations and wellbeing of New Zealand; and
   - The economic well-being of New Zealand.

3. Under the Intelligence and Security Act 2017, the agencies have four core functions:

   - Intelligence collection and analysis;
   - Provision of protective security services, advice and assistance;
   - Co-operation with other public authorities to facilitate their functions; and
   - Co-operation with other entities to respond to imminent threat.

4. New Zealand faces a range of national security threats. These include malicious cyber activity against organisations and individuals, foreign interference and espionage, violent extremism and terrorism, and insider threats. These threats are not unique to New Zealand: they also impact the wider Pacific region and our partners.

5. Threats to national security are often sophisticated, the potential impact is significant, and they are often secret or not widely known. To respond to them, under the Intelligence and Security Act 2017, our two agencies can use unique capabilities and form a key part of New Zealand's national security system.

6. Our intelligence capabilities allow us to identify, investigate, collect and report on these threats. We use these intelligence collection capabilities, supplemented by intelligence received from partners, to support government agencies in their operations and decision making, and to carry out their legislatively mandated functions. We also reduce the risk these threats pose through our protective security functions, working to improve information and physical security across New Zealand.

7. Our two agencies are closely aligned and share a number of functions to maximise our efficiency and effectiveness. We also work collaboratively with others. Often our role is to support New Zealand's law enforcement agencies, the New Zealand Defence Force (NZDF), the wider public sector, and a range of private sector organisations of national significance.

8. We also work with our partners in the Five Eyes, an intelligence sharing partnership made up of Australia, the United Kingdom, the United States, Canada and New Zealand, to ensure we have access to the capabilities, intelligence and skills we need to keep New Zealand safe.

9. Everything we do needs to be in accordance with New Zealand law and our international human rights obligations, and aligned with the requirements, spirit and values of New Zealand's public sector.

10. This briefing provides you with an overview of our operating context, structure, most significant challenges and empowering legislation. It sets out your statutory roles in relation to the GCSB and NZSIS. This briefing includes an introduction to our capabilities, as well as the threats New Zealand faces, and the specific ways in which we respond to them.

11. s9(2)(f)(iv) [redacted]

12. We will work with you and your office to provide further briefings on our functions and current operations.

Part One - About Us

13. GCSB and the NZSIS are two of the several agencies that come together to form New Zealand's national security community. This community is focussed on protecting a secure and resilient New Zealand—one that is a free, open and democratic society for future generations.

Government Communications Security Bureau - Te Tira Tiaki

14. GCSB is New Zealand's lead organisation for signals intelligence: collecting intelligence through electronic means such as accessing information infrastructures (known as SIGINT) and cyber security.

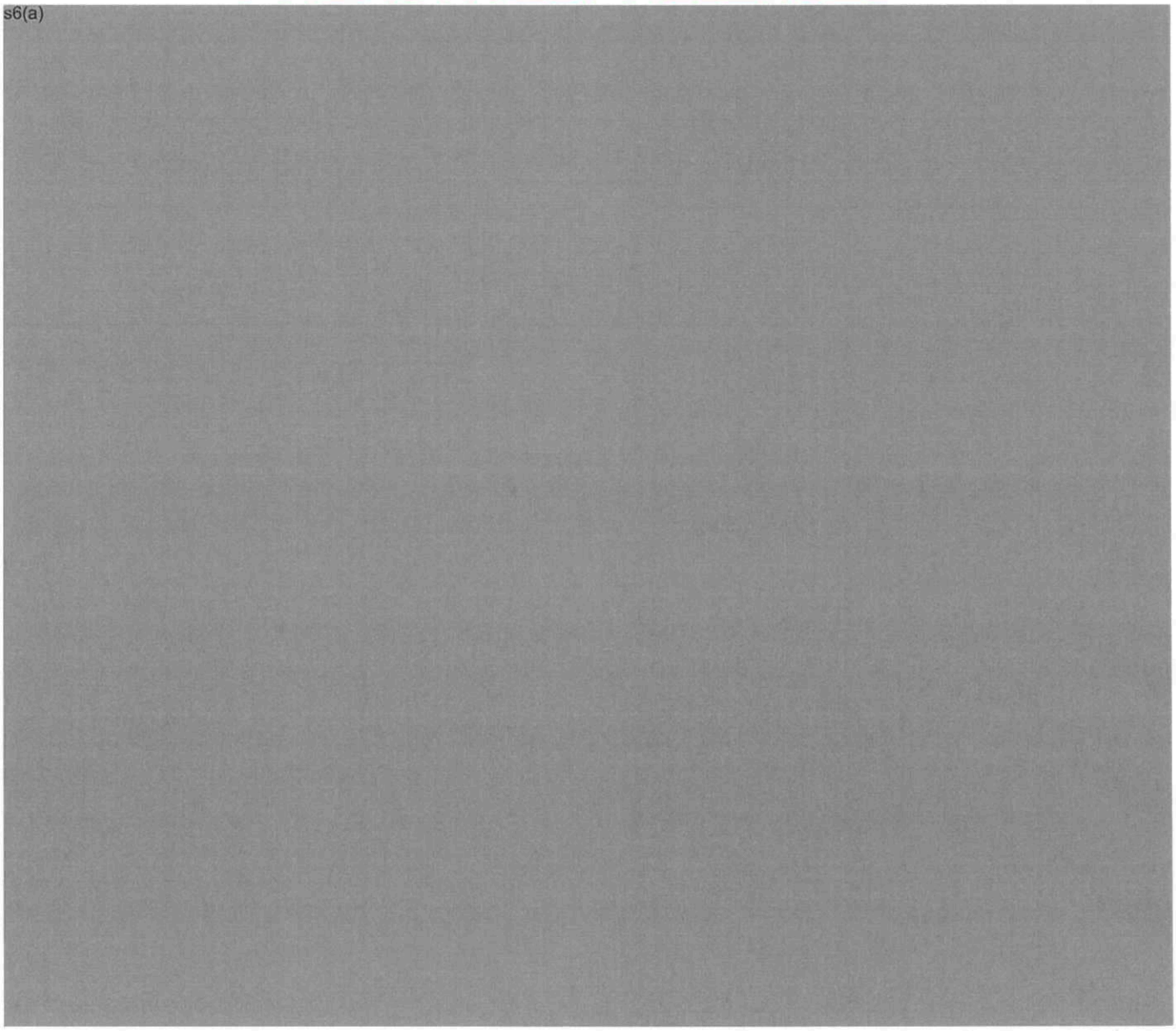
15. GCSB plays a crucial part in how New Zealand makes sense of the world and manages national security threats. Our mission is to equip our customers with the intelligence and cyber resilience necessary to forecast and successfully navigate New Zealand's changing strategic environment.

16. We operate in a complex and challenging threat environment. Our specialist knowledge and technical expertise repeatedly leads to reporting that provides unique insights to our domestic and international partners. s6(a) [redacted]

How does GCSB collect intelligence?

17. GCSB collects intelligence using several methods. These include but are not limited to:

s6(a)



20. GCSB collects against a wide range of National Security Intelligence Priorities (you can read more about these at paragraphs 209-211) but in particular: foreign intelligence and espionage, New Zealand's interests in the Indo-Pacific region, Pacific resilience and security, terrorism and violent extremism and transnational serious and organised crime. GCSB's role is to collect intelligence, develop intelligence products and ensure this information gets to the relevant international and New Zealand agencies to inform policy advice, operations and enforcement. These agencies can include Immigration New Zealand, New Zealand Customs Service, NZSIS, New Zealand Police, NZDF, Ministry of Foreign Affairs and Trade (MFAT) and the Ministry of Business, Innovation and Employment. GCSB also provides support to military operations.

National Cyber Security Centre

21. Under its information assurance and cyber security functions, the GCSB works to protect information systems and communications critical to New Zealand's national interests from sophisticated security threats. The National Cyber Security Centre (NCSC), a directorate within the GCSB, provides cyber security services and advice to New Zealanders to improve New

Zealand's resilience to cyber security threats. GCSB is the lead agency for information security for government. GCSB also acts as the New Zealand national authority for communications security – the technology and processes used to protect our most sensitive data through advanced encryption. Our work contributes to the cyber security of millions of New Zealanders.

22. GCSB provides its CORTEX programme to counter cyber threats to both public and private sector organisations of national significance. This involves GCSB using tools and threat information to protect these organisations from advanced persistent malicious software (malware). CORTEX cyber protection services operate a highly targeted range of capabilities and are only deployed with the express agreement of the organisation involved. s9(s)(f)(iv) [redacted]

23. GCSB works in partnership with internet service providers to deliver a capability called Malware Free Networks™(MFN). MFN is a scalable malware detection and disruption service which involves the NCSC generating, and near real-time sharing, cyber threat intelligence with consenting organisations. Since 2021, GCSB has disrupted over 1 billion malicious cyber events as part of MFN.

24. The NCSC provides cyber security incident response services to all New Zealanders – from individuals and small businesses through to large enterprises, government, and critical national infrastructure. This involves investigating and disrupting compromises as well as providing advice and coordination to resolve incidents. The NCSC's Incident Management unit is on call 24/7 to respond to cyber security incidents.

Government Chief Information Security Officer

25. The Director-General GCSB acts as the Government Chief Information Security Officer (GCISO). The GCISO drives system coherence to the government's approach to cyber security and aims to lift New Zealand's overall cyber resilience. The GCISO works closely with the other system leads, particularly the Government Chief Digital Officer and the Government Chief Data Steward to create trusted, secure and high-quality data, information and technology that enables our public service to deliver better outcomes for the wellbeing of New Zealand.

The Top Secret Network

26. The Top Secret Network (TSN) provides Top Secret services to s6(a government agencies. The TSN s6(a) [redacted] collaboration and communication between all TSN agencies. TSN services are provided by the GCSB, supported by a joint governance model with participating agencies.

27. s6(a) [redacted]

Top Secret Data Centre

28. In June 2022, Cabinet approved the delivery by GCSB of a new s6(a) [redacted] data centre to protect the New Zealand Intelligence Community's most valuable data and information. The data centre, Mātai, was completed in May 2025 and became fully operational in February 2026.

29. Work has progressed at pace to realise the intended benefits and achieve value from the Government's investment, s6(a) [redacted].

Location

30. The GCSB's head office is based in Pipitea House on Pipitea Street in Wellington. NCSC is located in Defence House. We have offices in three locations; Wellington, Auckland and Waihopai, near Blenheim, s6(a) [redacted]. We also have a high frequency radio interception and direction-finding station in Tangimoana, near Palmerston North. The data centre, Mātai, is located on the Whenuapai Air Force base in Auckland. As of 31 December 2025, GCSB had 583 full-time equivalent staff.

GCSB Senior Leadership Team

31. Andrew Clark is the Director-General of GCSB. He began this role on 30 October 2023.

32. He is the system lead for cyber security across the New Zealand Government, as the Government Chief Information Security Officer, reporting to the Digital Executive Board overseen by the Minister for Digitising Government. He is also a member of the New Zealand National Security Board[1].

33. Prior to his role at GCSB, Andrew spent 37 years in the NZDF and was the Chief of Air Force before he left. He held a number of other leadership roles at NZDF before this.

34. Andrew is supported by the GCSB Senior Leadership Team:

- s6(a) [redacted] – Deputy Director-General, Intelligence
- Catriona Robinson – Deputy Director-General, National Cyber Security Centre
- Monica Silverwood – Chief Legal Advisor
- Kate Pullar – Deputy Director-General, Strategic Direction*
- Nicky Haslam – Deputy Director-General Finance, Commercial and Property *
- s6(a) [redacted] – Deputy Director-General, Technology and Data*
- Shelly Thompson – Deputy Director-General, People and Capability*

* These roles are formally part of both agencies' leadership teams as part of our joint enabling functions.

New Zealand Security Intelligence Service - Te Pa Whakamarumaru

35. The NZSIS is a security intelligence agency responsible for identifying, investigating, assessing and with others, mitigating national security threats to New Zealand and New Zealanders. We do this

1 Chaired by DPMC, the National Security Board is a group of public sector chief executives who meet regularly to provide strategic leadership, oversee capability development and ensure that agencies' policies and activities align.

through our security intelligence, foreign intelligence and protective security services. We have four key impact areas:

- Countering espionage and foreign interference.
- Countering terrorism and violent extremism.
- Contributing to a secure, prosperous and resilient Pacific.
- Protecting people, information and assets.

How does the NZSIS collect intelligence?

36. NZSIS uses a range of collection methods such as physical surveillance, tracking devices, technical interception, listening devices, open source data analysis, tracking online activity and human intelligence activities (known as HUMINT). HUMINT can come from a range of sources, from covert human intelligence sources to private individuals who may offer information. Insights and reporting related to national security concerns and threats may also come through the overt external engagement the NZSIS undertakes with key sectors or through the NZSIS's online portal. The NZSIS can task GCSB to assist with our work, using their SIGINT capabilities.

37. The increasingly digital and data-driven world has impacted on both the information the NZSIS can access and the way NZSIS needs to work in order to deliver on our functions. To fulfil our mission NZSIS needs to access, analyse and use data that has become more complex, hidden and fragmented. Insights now increasingly come from our ability to acquire and make sense of different data, pulling together different information threads to connect dots to show where threats may lie.

38. If, through the course of our work, we discover intelligence of security concern, the NZSIS can share this information with appropriate agencies, such as the New Zealand Police, New Zealand Customs Service or Immigration New Zealand, in order for these agencies to disrupt such threats and mitigate risks to the public under their own mandates.

Our protective security leadership

39. The NZSIS has a statutory responsibility to provide protective security services, advice and assistance to the public sector. The Director-General of Security holds the role of Government Protective Security Lead (GPSL). Through this role, the Director-General provides protective security leadership, guidance, and support for chief executives, organisations, and systems across New Zealand.

40. The NZSIS is responsible for the Protective Security Requirements (PSR), which set out rules for governing and managing risk to the government's people, information and assets. The PSR Unit also provides a range of protective security guidance for business and the public, including on due diligence, travel, and foreign interference.

41. Implementing the PSR framework is mandatory for all public service departments, non-public service departments (NZDF and NZ Police), parliamentary agencies, and the Reserve Bank. A small number of additional agencies implement the PSR voluntarily.

42. Mandated and voluntary agencies report annually to the NZSIS on their compliance with the rules set out in the PSR. The framework for annual reporting has been significantly improved

over the past year, to make it more standardised and robust, and to incorporate reporting against Minimum Cyber Security Standards authored by the NCSC.

43. The NZSIS also supports other government agencies by providing expertise in areas such as personnel (i.e. insider investigations, clearance management, etc.) and physical security.

National security clearances

44. NZSIS assesses people's suitability to hold a national security clearance (known as security vetting) to determine who can be trusted with classified information, physical locations and access to systems. Security vetting focuses on identifying vulnerabilities that could be exploited and whether these can be mitigated. A national security clearance is not a substitute for an employing agency's recruitment, human resource management or security processes.

45. s6(a) [redacted]

s6(a) [redacted]

46. While traditionally primarily a domestic security intelligence agency, the NZSIS is increasingly focused on the Pacific. s6(a) [redacted]

Location

47. The NZSIS's head office is based in Pipitea House on Pipitea Street in Wellington. s6(a) [redacted] regional offices in Auckland, Christchurch, and overseas liaison offices. As of 31 December 2025, the NZSIS had 382 full-time equivalent staff.

NZSIS Senior Leadership Team

48. Andrew Hampton is the Director-General of Security. He has been in this role since April 2023.

49. Before joining the NZSIS, Andrew Hampton was Director-General of the GCSB for seven years.

50. Prior to joining the GCSB, Andrew spent much of his career in the justice sector, including Treaty settlement negotiations, courts administration and leading various significant change programmes. Senior positions he held in the justice sector include Director of the Office of Treaty Settlements, Deputy Secretary for Courts, and Deputy Chief Executive at the Crown Law Office. Andrew has also held senior leadership positions elsewhere in the state sector. He was Deputy Secretary and Director of the Secretary's Office at the Ministry of Education, and was also the Government Chief Talent Officer at the Public Service Commission.

51. Andrew is supported by the NZSIS Senior Leadership Team:

- Phil McKee – Deputy Director General, Intelligence

- Nick Marks – Deputy Director General, Protective Security
- Sharee Christensen – General Counsel
- Kate Pullar – Deputy Director-General, Strategic Direction*
- Nicky Haslam – Deputy Director-General Finance, Commercial and Property *
- s6(a) – Deputy Director General, Technology and Data*
- Shelly Thompson – Deputy Director General, People and Capability*

* These roles are formally part of both agencies' leadership teams as part of our joint enabling functions.

GCSB and the NZSIS work closely together

52. We frequently leverage our common intelligence functions and work together to detect, deter and disrupt specific threats to New Zealand's national security. NZSIS and GCSB's complementary intelligence capabilities cover a broad spectrum of intelligence sources.

53. For example, HUMINT activities may provide a lead or details of a target that enable a SIGINT access to be exploited, and vice versa. While this collaboration is essential, the disciplines remain unique, with distinct tradecraft, systems and expertise required to execute operations successfully.

54. As well as collaborating in the intelligence space, the agencies have a range of joint enabling functions.

Financial sustainability

55. In 2024/25, GCSB and NZSIS undertook a joint financial sustainability programme to ensure we remain efficient, financially sustainable, and well-equipped to face the evolving threat environment.s6(a)

56. The change process focused on maintaining core business, maximising alignment between the agencies and reducing unnecessary duplication. We reduced cost pressures through bringing more functions together as joint services shared by GCSB and NZSIS, reducing some of our leadership structures, disestablishing certain non-core functions and removing a number of vacancies. Changes were implemented in March 2025.

57. This was a separate process to operating efficiency savings already identified by the agencies as part of Budget 2024. The operating efficiency savings identified as part of Budget 2024 resulted in GCSB making savings of $7.62 million per year and NZSIS $3.44 million per year. The efficiency savings were achieved through identifying savings that could be managed without having a significant impact on current operational activity, such as spend on contractors and consultants, training and development, travel and reduced financial contingencies.

58. s6(a)

59. s6(a)

s6(a)

s6(a)

60. s6(a)

million.

61. s6(a) .

s9(2)(f)(iv)

62. s9(2)(f)(iv)

63. s9(2)(f)(iv)

Response to National Fuel Plan

64. In response to the Government's National Fuel Plan, the NZSIS and GCSB have completed an assessment of its fuel use and developed a plan to ensure vital and critical services can continue. This includes possible controls that can be implemented across the four phases of the National Fuel Plan.

65. The GCSB and NZSIS are not major consumers or holders of fuel. s6(a) [redacted]

66. We are working with MBIE to clarify whether the GCSB and NZSIS are considered as Priority Band A agencies under the National Fuel Plan.

Your statutory roles and responsibilities

The Intelligence and Security Act 2017 (ISA)

67. The ISA confers significant responsibilities on the Minister Responsible for the GCSB and the NZSIS. These include:

- Issuing intelligence warrants and removal and practice warrants (including in some cases in conjunction with a Commissioner of Intelligence Warrants);
- Approving a Director-General to issue business records directions and granting permission to access restricted information;
- Authorising others to receive intelligence;
- Authorising the provision of protective security services, advice and assistance by GCSB and NZSIS to any person/class of persons;
- Issuing Ministerial Policy Statements, a unique legislative tool which provides guidance to GCSB and NZSIS on lawful activities; and
- Providing a response to inquiries undertaken by the Inspector-General of Intelligence and Security (IGIS).

Warrants and authorisations

68. The GCSB and NZSIS use intelligence warrants to carry out much of their work. There are two types of intelligence warrants, as follows:

Type 1

69. A Type 1 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information about, or to do any other thing directly in relation to —

(a) any person who is—
  (i) a New Zealand citizen; or
  (ii) a permanent resident of New Zealand; or
(b) a class of persons that includes a person who is—
  (i) a New Zealand citizen; or
  (ii) a permanent resident of New Zealand.

Type 2

70. A Type 2 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information, or to do any other thing, in circumstances where a Type 1 warrant is not required.

71. Applications for Type 1 warrants are issued jointly by you as the authorising Minister, and a Commissioner of Intelligence Warrants, whereas Type 2 warrants are issued solely by the

authorising Minister. There are three Commissioners of Intelligence Warrants: Hon Robert Dobson KC (Chief Commissioner), Hon Karen Clark KC and Hon Brendan Brown KC. All have previously been High Court or Court of Appeal Judges.

72. The ISA also provides for the agencies to apply orally for an urgent intelligence warrant or apply to the Director-General for a very urgent authorisation in specific limited circumstances. Other warrants the agencies may apply for include a removal warrant, authorising the removal of devices previously installed under an intelligence warrant, and a practice warrant to enable testing (including maintaining or developing a capability) and training.

73. Intelligence warrant applications must meet certain criteria and warrants are issued to enable certain activities against individuals or classes of people or things. The activities include surveillance, interception, search, seizure and human intelligence.

74. Because of your statutory role, we regularly request meetings to seek warrants and authorisations. From time to time, fast-moving or urgent operational matters may mean we need to brief you at short notice, but otherwise we provide your office with warrant applications at least two working days prior to any meeting. If a Type 1 warrant is sought (one involving New Zealanders), a Commissioner of Intelligence Warrants will have already reviewed the application and will attend the meeting with you.

75. The Minister of Foreign Affairs is statutorily required to be consulted in relation to warrants that authorise activities likely to have implications for New Zealand's foreign policy or international relations. The Minister of Foreign Affairs receives written briefings from MFAT officials, where required, following input from the agency.

Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

76. TICSA requires network operators to ensure their public telecommunications networks have interception capability. It also requires network operators and services providers to assist the intelligence and security agencies to give effect to intelligence warrants.

77. Under Part 3 of TICSA, the Minister Responsible for the GCSB and the Director-General, GCSB have a range of responsibilities concerned with keeping New Zealand's telecommunications networks secure. TICSA requires public telecommunications network operators to notify the GCSB if they are planning a network change within certain areas of specified security interest. Notifiable changes include the purchase or acquisition of equipment or services, changes to network architecture, or changes in ownership or control.

78. If a significant network security risk is raised by a notification, the Director-General GCSB may refer the matter to the Minister Responsible for the GCSB for a direction to prevent, reduce, or mitigate the identified network security risk. TICSA sets out a process for making such a direction, which includes consultation with the Minister for Media and Communications and the Minister of Trade.

79. s6(a) [redacted]

Outer Space and High-altitude Activities Act 2017 (OSHAA)

80. The Outer space and High-altitude Activities Act (OSHAA) 2017 provides a regulatory framework to manage any risks to New Zealand's national security and interests from outer-space and high-altitude activities.

81. Payload permits are granted by the Minister Responsible for the Outer Space and High-altitude Activities Act 2017 and administered by the New Zealand Space Agency. The Space Activities Risk Assessment Group (a New Zealand Intelligence Community working group comprising GCSB, NZSIS and NZDF) undertakes a national security risk assessment in order to inform your consultation with the Minister Responsible for OSHAA. You will receive briefings informing you of the outcome of national security risk assessments for payload permits applied for under the OSHAA.

82. Amendments in 2025 updated OSHAA to include regulation of ground-based space infrastructure (GBSI). The GCSB and NZSIS are supporting the New Zealand Space Agency with implementing the national security components of this new regime.

Overseas Investment Act 2005

83. Overall, foreign direct investment in New Zealand is positive for our economy. However, occasionally foreign investment can involve risks, including national security risks that need to be balanced with the benefits.

84. The Overseas Investment Office (the regulator) provides advice to the responsible Minister regarding transactions. The NZSIS and GCSB provide advice to the regulator regarding any national security risks associated with proposed overseas investments.

Radiocommunications Act 1989

85. The GCSB and the NZSIS provide advice to the Minister for Economic Development on the outcome of national security risk assessments in relation to issuing licenses for satellite ground stations. This is based on a direction under section 112 of the Radiocommunications Act 1989, which authorises the Radio Spectrum Management team within MBIE to seek such advice. The Space Activities Risk Assessment Group coordinates advice provided in relation to these applications.

Part Two – Threat environment and our response

86. This section outlines the main national security threats New Zealand faces and how the agencies are seeking to keep ahead of the threats. The global threat environment continues to deteriorate, largely driven by less stable relationships between states and increasing levels of polarisation and grievance.

87. New Zealand faces a range of national security threats. These include malicious cyber activity against organisations and individuals, foreign interference and espionage, violent extremism and terrorism, and insider threats. These threats are not unique to New Zealand: they also impact the wider Pacific region and our partners.

88. Many of the threats faced by New Zealand originate from actors who go to great lengths to hide their activities. Sophisticated security awareness and counter-intelligence capabilities are

increasingly not solely the purview of state sponsored intelligence officers. Both state sponsored and criminal cyber actors use technically complex means to exploit their targets and avoid identification. Likewise, groups and individuals with extremist ideologies can cover their tracks through the use of readily available encrypted communications previously unavailable to them. Artificial intelligence, which is becoming more accessible and easier to use, can further enable threat actors and widen the scope and scale of their harmful activities against New Zealand.

89. It is for these reasons that New Zealand's security and intelligence agencies require advanced capabilities, techniques and skill sets to acquire intelligence from various sources. Information relating to our capabilities and operations are kept secret under the highest levels of security and classification. A target's knowledge that they are or are not of interest to the agencies, or knowledge of the capabilities of the New Zealand security and intelligence agencies, will invariably alter that target's behaviour. Should a foreign state gain unauthorised access to such information, it could seriously compromise New Zealand's defence, security and international relationships.

s6(a) [redacted]

90. The NZSIS and GCSB are monitoring the unfolding situation in Iran and the potential impact on our local threat environment. There is no change to the national terrorism threat level or our current risk profile as a consequence of the conflict. Another terrorist attack is still assessed as POSSIBLE, however the situation could change with little warning. s6(a) [redacted]

91. s6(a) [redacted]

92. s6(a) [redacted]

93. s6(a) [redacted]

94. s6(a) [redacted]

95. s6(a) [redacted].

96. s6(a) [redacted]

97. s6(a) [redacted]

98. s6(a) [redacted]

Geostrategic competition

99. Geostrategic competition is where states seek to advance competing visions for regional and global orders. We have seen this return to the forefront between the major powers, which is making the global and regional security environment more complex and unpredictable.

100. There are clear implications for New Zealand and our home region when geopolitical tensions become more intense. New Zealand is a small, export nation which relies on stable international rules-based order.

101. The increase in geostrategic competition and associated weakening of the rules-based order is seeing more states revert to foreign interference, espionage and cyber-attacks to achieve their objectives. Such activity is occurring in our region and within New Zealand.

102. Rapid technological change, despite its many benefits is being used by malicious state and non-state actors in ways that threaten our national interests.

103. The Indo-Pacific region has seen increased geostrategic competition and we have a role in supporting the resilience of our regional partners to ensure the stability and prosperity of the region.

104. The increasingly complex geostrategic environment means the pivotal role the agencies play in providing both intelligence and protective security services will only become more important.

Detecting and monitoring foreign interference and espionage activities in New Zealand

105. Foreign interference is an act by a foreign state, often through someone working on its behalf (a proxy), intended to influence, disrupt, or subvert New Zealand's national interests by deceptive, corruptive, or coercive means. Espionage refers to clandestine activities undertaken to acquire non-public information or materials for the benefit of a foreign state.

106. Foreign interference and espionage are closely linked and mutually supportive, and pose a significant threat to New Zealand's interests. Some foreign states target New Zealand to advance

their political, economic and military advantage by attempting to steal New Zealand's secrets or by co-opting individuals who are (or are close to) key decision makers. The NZSIS has also observed foreign interference activities targeting our local government, academic, and media sectors. s6(a) [redacted]

107. Transnational repression is a common form of foreign interference detected in New Zealand. The main target of transnational repression are our migrant and well-established diaspora communities who may be viewed as dissidents by a foreign state. These communities are targeted by foreign states through harmful activities designed to intimidate them and suppress their rights and freedoms in New Zealand.

108. Last year, the Crimes Act 1961 was amended to include new foreign interference offences and modernised espionage and wrongful communication offences. This allows New Zealand Police to investigate allegations of foreign interference and espionage and pursue charges where appropriate.

109. Espionage and foreign interference present substantial challenges for the intelligence community. State intelligence apparatuses are often well resourced, practised in their tradecraft and security practices, and supported by co-optees within New Zealand who are either compromised or motivated by nationalist duty. s6(a) [redacted].

110. s6(a) [redacted].

Countering the threat of violent extremism and terrorism

111. The global threat environment continues to deteriorate. Some overseas partners have experienced increased threats and realised attacks. Following the terrorist attack at Bondi Beach in Sydney on 14 December 2025, the NZSIS immediately stood up an operation to understand how the Bondi attack might impact the New Zealand threat environment. We also provided support as required to our Australian and New Zealand Police colleagues.

112. New Zealand's violent extremism threat environment has remained largely consistent over the past year. In February 2026, the National Terrorism Threat Level was set at POSSIBLE; a terrorist attack is assessed as possible. A small number of individuals in New Zealand continue to express intent to undertake an act of violent extremism, some of whom almost certainly have access to the basic capability to do so. The most plausible domestic attack scenario remains a lone actor mobilising to violence with little to no intelligence forewarning.

113. There is no one ideology which dominates in the New Zealand threat environment. In our investigations, we see White Identity-Motivated Violent Extremism, Faith-Motivated Violent Extremism and individuals motivated by radical political ideologies or online conspiracy theories. Individuals fixated on violence with mixed, unstable or unclear (MUU) ideological perspectives remain a particular concern. These individuals are harder to detect and disrupt and often have co-existing vulnerabilities that which can hinder effective disengagement. We continue to see young and vulnerable people at risk of becoming radicalised to a violent extremist ideology online.

114. The NZSIS advocates for an all of society approach to identifying and preventing violent extremism and terrorism. Raising public and community awareness of the threat of violent extremism and terrorism is important as members of the public may see concerning behaviour such as early signs of radicalisation. We encourage the public to report information of concern to the NZSIS or the New Zealand Police.

Partnering for cybersecurity

115. The interests and activities of a range of malicious cyber actors in cyberspace, both state and non-state, threaten to exploit cyber security vulnerabilities of New Zealand. These threats come in many forms, continually adapting to advancements in new technology and security measures. Cyber security is a rapidly evolving domain.

116. s6(a) [redacted] In 2023 and 2024, New Zealand joined with like-minded partners in releasing public attribution statements calling out malicious cyber activity from Russia and PRC, respectively. You can read more about public attribution statements at paragraphs 154-156.

117. Cyber criminals impact New Zealand for a range of reasons, including financial and political, through ransomware, hacktivism, and extortion activity. This activity can be carried out from anywhere in the world and is often carried out indiscriminately or without a specific intent to target New Zealand. Cyber criminal actors may collaborate with states to obfuscate state-aligned activity, and use a range of sophisticated and unsophisticated techniques, such as spear phishing.

118. The NCSC disrupts malicious cyber activity from impacting its customers' environments by blocking harmful activities through our active disruption capabilities. We intervene to remove malicious cyber actors from victim networks and support affected organisations. We partner with New Zealand industry to deliver MFN and to drive system-wide improvements. A range of partners now provide MFN as a service to customers, meaning that MFN provides coverage to the majority of New Zealanders.

Pacific regional security

119. What happens in the Pacific has a fundamental impact on New Zealand's own national security, prosperity and identity. New Zealand and our Pacific neighbours exist in a security environment that is becoming increasingly challenging for governments to navigate.

120. s6(a) [redacted]

121. s6(a) [redacted]

122. s6(a) [redacted]

123. s6(a) [redacted]

124. s6(a) [redacted]

125. s6(a) [redacted]

126. GCSB works with Pacific Island countries on raising their cyber resilience in a sustainable manner. GCSB supports Pacific Island countries with awareness raising efforts and educational campaigns, delivers training, and supports the development of national cyber security functions as well as providing support to the Pacific Cyber Security Operational Network (PaCSON), a multinational cyber security forum.

127. NZSIS works with a number of Pacific partners s6(a) to share expertise on how to build and implement protective security frameworks that help protect people, assets and information from harm. The aim of this engagement is to support Pacific partners to implement their own bespoke arrangements that respond to their individual security environment and needs.

Part Three - Working with others

128. As part of New Zealand's national security community, the GCSB and NZSIS work together with a range of agencies and organisations to help enhance New Zealand's national security. This section details many of our regular and enduring relationships across government, private sector and the community, as well as the importance of the Five Eyes partnership.

Government partners

DPMC's role in the NZIC

129. Our agencies work closely with the National Security and Resilience Group (NSRG) in DPMC, which holds a collaborative leadership role within the national security community. The NSRG leads and provides strategic coordination on national security policy issues, including cyber security policy.

130. The NSRG's policy directorate operates in a similar way to how the Ministry of Justice provides policy advice about the operations of the New Zealand Police. The National Security Policy and Coordination Directorate provides policy advice about the roles and functions of GCSB and NZSIS, to the Minister for National Security and Intelligence and to you as the agencies' responsible Minister.

131. The NSRG leads the development and coordination of the National Security Strategy, National Cyber Security Strategy, National Security Intelligence Priorities, and Ministerial Policy Statements.

132. The National Assessments Bureau (NAB), which forms part of the NSRG, provides strategic assessments to the Prime Minister, senior Ministers, and senior officials on international developments and events relevant to New Zealand's interests. The Director of NAB is responsible for coordinating intelligence assessment and promoting standards of intelligence assessment across the national security community.

Working with NZDF

133. GCSB and NZSIS work in partnership with NZDF to provide support to military operations, to provide force protection to New Zealand forces deployed overseas. s6(a)

s6(a) [redacted]

134. s6(a) [redacted]

135 s6(a) [redacted]

Working with law enforcement

136. NZSIS and GCSB work closely with a number of New Zealand law enforcement agencies, most prominently the New Zealand Police and the New Zealand Customs Service.

137. NZSIS and New Zealand Police are joint operational system leads for counter-terrorism and this partnership is essential for our work to identify, monitor, mitigate and disrupt violent extremist and terrorist threats. We continue to strengthen our partnership so that we can more effectively leverage these powers. There are NZSIS and New Zealand Police staff co-located s6(a) [redacted] and s6(a) [redacted] work together on a daily basis.

138. GCSB contributes to efforts to counter transnational serious organised crime, with a focus on illicit drug trafficking. GCSB works with New Zealand Customs Service and NZDF as part of Operation Kiwa to disrupt and deter transnational serious organised crime networks targeting New Zealand and our region. Our combined capabilities deliver enhanced maritime intelligence, supporting NZDF operational activity and Customs enforcement, to defend New Zealand and our Pacific partners from organised crime networks.

139. NCSC and New Zealand Police have an exchange programme to support analysis of cyber incidents and promote greater inter-operability between the two agencies for cyber-dependant crime.

140. Both the GCSB and NZSIS receive leads from international partners and pass these on to the appropriate domestic agencies.

The Combined Threat Assessment Group

141. The Combined Threat Assessment Group (CTAG) is an interagency group hosted and led by the NZSIS. CTAG provides independent assessments to inform the national security community and wider government agencies of the physical threat posed by terrorism to New Zealanders and New Zealand's interests domestically and overseas.

142. Alongside NZSIS staff, CTAG includes representatives from NZDF, New Zealand Police, Department of Corrections, the Civil Aviation Authority and the National Assessments Bureau, with funding contributions from MFAT and the New Zealand Customs Service.

143. As the host agency, the NZSIS brings together insight from across government agencies to ensure that the Director-General of Security has the best advice to set the national terrorism threat level

appropriately. The national terrorism threat level informs national security risk management and decision-making processes. CTAG also prepares threat assessments on a wide range of domestic and global terrorism threat issues.

Border protection

144. NZSIS contributes to the management and protection of New Zealand's border by identifying and investigating national security threats in support of New Zealand's border security agencies, and in support of immigration decision making. NZSIS does this by providing advice about persons who attempt to enter New Zealand, or who apply for residency status and might represent a threat to national security. Between Immigration New Zealand and NZSIS, we identify travellers with links to international extremist groups, foreign interference and espionage activities or the proliferation of weapons of mass destruction technology.

International partners

145. International intelligence-sharing arrangements are vital to New Zealand's national security and fundamental to how the GCSB and NZSIS carry out their functions. New Zealand could not deliver our security and intelligence activity alone. Our most significant relationship is as part of the Five Eyes partnership, but the global nature of threats is increasingly requiring engagement with a far broader number of partners.

146. At a technical level, the Five Eyes relationship provides access to advanced technology and tradecraft techniques that New Zealand could not develop on its own. We also get access to skills, training programmes, professional and security standards that would be difficult and expensive to source, or source at scale, in New Zealand.

147. s6(a) [redacted]

148. As outlined earlier, we work closely with our Pacific partners to support regional security.

149. Under Ministerial authorisation, we also share intelligence with a range of other international counterparts, s6(a) [redacted]

150. Robust policies and processes remain in place to ensure any intelligence cooperation with international partners, s6(a) [redacted], is undertaken in accordance with New Zealand's own national security priorities and our own legislation. This includes regular human rights assessments.

s6(a) [redacted]

151. s6(a) [redacted].

152. s6(a) [redacted]

s6(a)

153. s6(a)

Public attribution statements

154. Public attribution statements are a tool used internationally to respond to malicious state-sponsored cyber activity. The key objective of public attribution is to deter states from engaging in this activity by strengthening international understanding of unacceptable state behaviour online. New Zealand has a vested interest in upholding the framework of responsible state behaviour in cyberspace and will publicly attribute when it is in our interests to do so.

155. The GCSB, acting on direction from responsible Ministers, has a history of joining like-minded partners in publicly calling out malicious cyber activity. Incidents that may result in an attribution include a partner's request for New Zealand to join an attribution statement, or an advisory alerting the public to a major cyber compromise affecting a New Zealand based entity.

156. If partners request support for a public attribution, the GCSB will engage in interagency consultation and provide you with the necessary advice to determine whether to direct the GCSB Director-General to make the attribution. Officials follow established processes to assess these requests, including engaging Ministers when necessary.

Private sector partners

157. New Zealand's private sector is well placed to benefit from the unique insights from the intelligence agencies on national security threats they may face. The NZSIS's Security Threat Environment report and the GCSB's NCSC Annual Cyber Threat report contain information that will be helpful for corporates to manage their own risk.

158. The private sector is key in the GCSB's mission towards a cyber-resilient New Zealand. Providing high-quality cyber threat information that they can readily use to help protect their customers, in tandem with other commercial products, makes a real difference in the long term. As outlined earlier, GCSB works in partnership with internet service providers to deliver MFN.

159. NCSC's advice and services are not limited to national security – cyber security also encompasses digital transformation, emerging technology and critical infrastructure resilience. The NCSC partners with industry on a range of areas such as incident response, to provide complementary skills and services, and with vendors in the supply chain to ensure that cyber resilience is a key consideration in their products and services.

160. Both agencies have best practice protective security advice on their websites that can be used to inform and improve other organisations' security posture. For example, in 2024 the NZSIS and the NCSC, along with the Five Eyes, launched security guidance to help protect emerging technology companies from a range of threats. The NZSIS also regularly engages with the private sector, with a focus on technology and critical infrastructure. We aim to build a security culture

in New Zealand where best practice is adopted and concerning activities or behaviours of national security significance are reported.

Community and sector engagement

161. Protecting our national security is increasingly becoming a task we cannot afford to do alone. Information from members of the public could be vital for helping us to disrupt a potential threat. In order to facilitate that flow of information, we realise the importance of informing New Zealanders about the threats we face and talking about the types of behaviours that are concerning.

162. Since the terrorist attack in Christchurch on 15 March 2019, we have significantly increased our engagement with a range of communities to identify and discuss shared national security concerns. The volume of engagements has increased over the last three years, averaging 80 recorded engagements per month. In 2025, NZSIS undertook a total of 955 engagements, approximately half of which took place with communities or entities across New Zealand.

163. NZSIS work with the Muslim Advisory Group and the Community Security Group which remain key forums for collaboration, including community-based engagements and youth events, and to share and receive insights with faith-based communities.

164. The NZSIS also engages with a wide range of communities and sectors, including; the private sector; education and research (with a focus on the tertiary sector for foreign interference and espionage and the secondary sector for violent extremism and terrorism); ethnic and faith-based communities; Tangata Whenua; local Government and emergency services and response.

165. NZSIS are working on increasing engagement with:

- s6(a) [redacted]
- young people due to their heightened vulnerability to violent extremism and online radicalisation
- the private sector to strengthen resilience to foreign interference, insider threat and espionage.

166. GCSB works with community partners to promote good cyber security practice and support New Zealanders to be more cyber resilient.

167. The agencies seek to be honourable Treaty partners who deliver national security outcomes in accordance with Te Tiriti o Waitangi. We are committed to working with Māori on a range of national security issues. s9(2)(ba)(i) [redacted] NZSIS is also working with a Māori Reference Group to develop a resource to support Māori businesses to build resilience against national security threats.

Contributing to the public conversation about national security

168. The agencies have responded to shifting threats and increased public demand for information about national security. Through the Department of the Prime Minister and Cabinet's (DPMC)

annual National Security Survey and the findings from the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain, we know that the public want to be better informed about security risks.

169. By routinely being more open about national security, we can develop a greater understanding and help the public to be better placed to manage risks. Below are some examples of how we regularly communicate with the public about national security. We will engage with you and your office in the lead-up to these publications and public statements.

National Terrorism Threat Level

170. While constantly under review, the National Terrorism Threat Level is formally reviewed annually through a National Terrorism Threat Level Assessment. The Director-General of Security is responsible for setting the National Terrorism Threat Level, informed by CTAG. The primary purpose of the threat level is to inform relevant government agencies so their security plans and settings are appropriate to the assessed threat. It also provides an opportunity to share information with the public on New Zealand's threat environment. The threat level is published on the NZSIS website.

171. In February 2026, the Director-General set the threat level at POSSIBLE; Terrorist attack is assessed as possible. This year, CTAG implemented new language to describe the threat levels. The updated language is intended to better articulate the threat environment to government stakeholders and the public, helps address feedback from communities and aligns with language used by our Five Eyes partners.

Annual Security Threat Environment report

172. The NZSIS publishes an annual Security Threat Environment assessment to inform the public about national security threats facing New Zealand, including violent extremism, foreign interference, espionage and insider threats. The report also contains protective security guidance to individuals and organisations on how to reduce or otherwise treat national security risks. By providing greater security awareness and protective security we hope to promote improved understanding and transparency and support better security outcomes in New Zealand. We are planning to release the next edition in August 2026.

Know the signs: a guide for identifying signs of violent extremism - Kia mataara ki ngā tohu

173. The NZSIS has researched the common behaviours and activities displayed by violent extremists who mobilise to violence. This research drew on case studies from New Zealand dating back to 2006, of violent extremists that were motivated by a variety of ideologies. The research was validated by case studies from around the world and led to the development of the NZSIS Terrorism Indicator Framework. The work evolved to become the NZSIS's first-ever public guide to help New Zealanders identify behavioural signs of violent extremism*: Know the signs: a guide for identifying signs of violent extremism - Kia mataara ki ngā tohu*, which was published in 2022.

174. The NZSIS uses the guide as an engagement tool to work with stakeholders and communities, including schools, NGOs and community service providers, on how to identify the signs and report behaviour of concern. This tool has been adapted and used to support psychologists, social workers and carers to identify early signs of radicalisation in vulnerable people. If these

signs are reported at an early stage, it could support the disruption of someone on the pathway to radicalisation and the mobilisation to violence.

Annual Cyber threat report

175. NCSC releases an annual cyber threat report. This report provides an overview of New Zealand's cyber threat landscape and the key insights for security professionals. The most recent cyber threat report was published on the NCSC website on 10 December 2025.

Cyber attributions

176. GCSB, through the NCSC, conducts technical attributions of malicious cyber activity and provides this (usually at a classified level) to the Government. The Government may draw on the NCSC's technical attribution – as part of an all-of-government process – and use this information to publicly call out a malicious cyber actor.

177. GCSB also joins our partners in publicly calling out malicious cyber activity and these are published on the NCSC website. New Zealand only attributes malicious cyber activity when it is in our national interest to do so.

Cyber security advisories

178. GCSB also supports New Zealand's organisations to respond to changes in the cyber and technology threat landscapes by publishing a range of technical cyber security advisories and alerts regarding potential or current threats. Security advisories share information about specific vulnerabilities or types of malicious cyber activity seen targeting local networks. Advisories often incorporate technical indicators of compromise and mitigation advice security teams can use to strengthen their defences. Sometimes these advisories may name states or actors associated with this activity. These instances are assessed on a case-by-case basis with both MFAT and DPMC and we will inform you if there are significant risks to doing so.

Cyber smart week

179. Each October NCSC runs a Cyber Smart week campaign to raise awareness of cyber security issues and encourage New Zealanders to adopt good cyber security practices.

Part Four – Upcoming matters

180. The following section provides context on upcoming key issues, events or decisions.

Warrants and authorisations

s6(a)

181. s6(a)

s6(a)

182. s6(a)

- [redacted] s6(a) [redacted]

- [redacted]

183. s6(a) [redacted]

s6(a) [redacted]

184. s6(a) [redacted]

185. s6(a) [redacted].

s6(a) [redacted]

186. s6(a) [redacted]

187. s6(a) [redacted].

188. s6(a) [redacted].

s6(a) [redacted]

189. s6(a) [redacted]

190. s6(a) [redacted]

Events

Support to the 2026 General Election

191. New Zealand's democratic system relies on a safe and secure general election. There are a number of risks that may threaten the delivery of the election and we play a role in mitigating those with a national security nexus, namely foreign interference, violent extremism and malicious cyber activity. We identify and report on such threats, and work in close cooperation with other government agencies to address them. Public confidence in the electoral process remains a critical objective of all agencies involved in supporting the General Election.

192. s6(a) [redacted]

193. We have no role in monitoring political discussion. We are obliged by law to be politically neutral and respect the right to freedom of expression. Mis and disinformation form part of the information environment and can intensify over an election period. We remain alert to disinformation that may emanate from a foreign state or a violent extremist group.

s6(a) [redacted]

194. s6(a) [redacted]

195. s6(a) [redacted]

196. s6(a) [redacted]

197. s6(a) [redacted]

198. s6(a) [redacted]

Policy work with other agencies

199. The GCSB and the NZSIS play a significant role in providing advice on, and input into, a range of policy work led by other agencies. While other agencies are responsible for managing national security risks within their portfolio responsibilities, we play an important role in informing the Government of the threat environment, providing advice on protective and cyber security, and conducting national security assessments to help mitigate these risks. We have a particular interest in ensuring that legislative and other changes reflect national security interests.

Intelligence and Security Act amendments

200. The Intelligence and Security Act 2017 requires periodic reviews and the first review was completed on 31 January 2023. The policy response to the Review is led by DPMC. s9(2)(f)(iv) [redacted]

201. s9(2)(f)(iv) [redacted]

202. s9(2)(f)(iv) [redacted]

Targeted review of Terrorism Suppression Act 2002

203. The Ministry of Justice is currently undertaking a targeted review of the Terrorism Suppression Act 2002 (TSA). The TSA was originally passed following the terrorist attacks in the United States on September 11 2001, and was designed to address the prevailing terrorist threat at that time, organised groups. The TSA is no longer fit for purpose and does not respond to the terrorist environment in New Zealand.

204. To address this, the NZSIS and the GCSB have been supporting the TSA targeted review to ensure it provides the counter-terrorism sector with the tools it needs to address the threat environment, including proposed new offences. s6(a) [redacted]

205. s6(a) [redacted]

s6(a) [redacted]

206. s6(a) [redacted]

[redacted]

s6(a) [redacted]

207. s6(a) [redacted]

National Cyber Security Strategy

208. Cabinet recently signed off on a new National Cyber Security Strategy and Critical Infrastructure Discussion Document that was developed by DPMC. The Strategy contains an Action Plan detailing what the Government will do to progress cyber security in New Zealand from 2026-2030. The Critical Infrastructure discussion document is seeking feedback from the public, commencing 27 February 2026, on enhancing the cyber security of critical infrastructure.

Part Five - Accountability

National Security Intelligence Priorities

209. The National Security Intelligence Priorities – Whakaarotau Marumaru – define where intelligence should support government to make informed decisions about national security.

210. The 2023 National Security Intelligence Priorities were approved by Cabinet in June 2023. They help us to understand and take action on the national security issues, threats, and drivers of instability set out in Secure Together, Tō Tātou Korowai Manaaki: New Zealand's National Security Strategy 2023 – 2028.

211. The National Security Intelligence Priorities are:

1. Economic security
2. Emerging, critical and sensitive technology
3. Foreign interference and espionage
4. Malicious cyber activity
5. Maritime and border security
6. National security implications of climate change
7. National security implications of disinformation
8. New Zealand's strategic interests in the Indo-Pacific region
9. Pacific resilience and security
10. Space security
11. Strategic competition and the rules-based international system
12. Terrorism and violent extremism
13. Threats to New Zealanders overseas
14. Transnational serious and organised crime.

Ministerial Policy Statements

212. Provided for by the ISA, Ministerial Policy Statements (MPSs) are a mechanism that enables the responsible Minister to set out their expectations about the appropriate conduct of lawful activities by the GCSB and NZSIS. As MPSs only apply to lawful activities, they do not serve to

authorise the activities but rather provide guidance as to the parameters of appropriate behaviour.

213. There are eleven MPSs (required under sections 206 and 207 of the ISA):

- Information assurance and cybersecurity activities
- Assumed identities
- Legal entities
- Collecting human intelligence
- Conducting surveillance in a public place
- Publicly available information
- Section 121 requests
- Information management
- False or misleading representations about employment
- Road user rule exemption
- Cooperating with overseas public authorities.

214. The MPSs are required to be reviewed every three years and were reissued without change in February 2025. DPMC intends to review all the MPSs s9(2)(f)(iv) [redacted]. The responsible Minister may amend, revoke or replace a MPS at any time (subject to the consultation requirements under the ISA)[2]. You are also able to issue MPSs to provide guidance about any additional matter.

GCSB's and NZSIS's oversight and accountability framework

215. The ISA sets out the key parts of GCSB's and NZSIS's oversight and accountability framework. Through independent oversight, a balance is struck between the secrecy necessary for the agencies to operate effectively and the public's expectations of accountability and transparency. Our overarching oversight and accountability framework has multiple layers, which are described below.

Executive / Ministerial

216. The Minister Responsible for the GCSB and NZSIS oversees day-to-day business and approves warrant applications brought by the agencies.

217. The Minister for National Security and Intelligence oversees the national security community. There is a legislative requirement to review the intelligence agencies and the ISA five years after the commencement of the ISA and periodically thereafter.

218. As outlined earlier in this briefing, the first review of the ISA was completed on 31 January 2023. The Government response to the report is being jointly led by the Prime Minister, as Minister for National Security and Intelligence and the Minister Responsible for the NZSIS and the Minister

---

[2] When issuing, amending, revoking or replacing a Ministerial Policy Statement, the responsible Minister must consult with the Inspector-General of Intelligence and Security, any other Minister of the Crown whose area of responsibility includes an interest in the proposed Ministerial Policy Statement, or any other person the Minister considers appropriate.

Responsible for the GCSB. DPMC administers the ISA and is the lead agency for responding to the review. We are supporting them with this work.

219. The Cabinet Foreign Policy and National Security Committee (FPS) is chaired by the Prime Minister and considers matters on foreign policy, external relations and the national security and intelligence sector.

Parliamentary

220. The Intelligence and Security Committee (ISC) is our parliamentary oversight committee. The Committee is established by the ISA, with members appointed by the Prime Minister and Leader of the Opposition, in consultation with other party leaders in Parliament. The functions of the ISC are outlined in section 193 of the ISA.

221. Accountability documents ordinarily presented to the House of Representatives (annual reports, Estimates of Appropriations, statements of strategic intent) are instead provided with classified material to the ISC.

Inspector-General of Intelligence and Security (IGIS)

222. The IGIS is a statutory officer providing independent external oversight and review of the intelligence and security agencies.

223. The IGIS' work involves:

- Investigating complaints about the NZSIS and the GCSB
- Conducting inquiries and reviews into the activities of the agencies
- Reviewing all warrants and authorisations issued to the intelligence and security agencies
- Receiving protected disclosures relating to classified information or the activities of the intelligence and security agencies
- Providing advice on matters relating to oversight of the intelligence and security agencies, including input into the development of relevant government policy

224. The full functions of the IGIS are detailed in section 158 of the ISA.

225. The Minister Responsible for the GCSB and the NZSIS, the Prime Minister, or the ISC can ask the IGIS to conduct an inquiry into the matters provided for in the ISA; however the IGIS mostly initiates inquiries on their own initiative.

226. The Inspector-General will generally conduct an inquiry if a matter requires in-depth investigation, such as interviewing witnesses. The IGIS may also decide to conduct an inquiry into a complaint received about the agencies.

227. A review will generally be less formal than an inquiry and will usually involve the IGIS selecting an area of an agency's work for examination and assessment.

228. A classified report is produced at the end of an inquiry or review and provided to the relevant agency and the Minister responsible for the agency. The report may include findings and recommendations about actions that the IGIS considers the agencies should take. A public report

will also usually be prepared that does not involve classified information, for publication on the IGIS website.

229. The IGIS prepares an annual work programme which indicates the areas the IGIS intends to review over the following 12 months. The annual work programme for 2026-27 will be released around June 2026.

230. The IGIS is supported to perform their role by a statutorily appointed Deputy IGIS and a team of approximately six employees. The current Inspector-General is Brendan Horsley. He was appointed in June 2020 for a five year term, and reappointed in 2025 for a further term of three years.

General

231. The Minister and the agencies are subject to the courts, including through judicial review. The agencies are also subject to oversight and review by:

- The Privacy Commissioner;
- The Ombudsman; and
- The Auditor-General.

Part Six – How we will support you

232. This section contains some suggestions based on current practice, for how we could provide day-to-day support to your office.

Directors-General

233. We are available at all times. We will inform you of any travel commitments that we have and when acting arrangements are in place.

Regular meeting schedule

234. The GCSB and NZSIS currently hold s6(a) meetings with the responsible Minister, with the agenda reflecting joint and agency-specific items. These meetings are attended by the respective Director-General and members of our Senior Leadership Teams, as well as specialist briefings as required. The meetings need to be held in s6(a) to ensure our classified information is protected. The meetings cover emerging policy and operational issues, matters coming before Cabinet committees, upcoming media issues, and matters relating to the organisational health of the agencies. They are also used to brief the Minister on warrant applications. We recommend these arrangements continue.

235. s6(a)

Responsibilities to the Prime Minister, Leader of the Opposition and Ministers

Prime Minister

236. We have responsibilities to the Prime Minister, as Minister for National Security and Intelligence. Our relationship with the Prime Minister is independent of their portfolio responsibilities for DPMC's national security function.

237. On occasion we provide briefings to the Prime Minister. We have hosted the Prime Minister in our head office s6(a) . s2(g)(i)

Leader of the Opposition

238. We have statutory responsibilities under the ISA to the Leader of the Opposition. This requirement strengthens bipartisan understanding of national security issues and reinforces the political neutrality of the security and intelligence agencies.

239. In accordance with our statutory responsibilities, our recent practice has been to brief the Leader of the Opposition s6(a) . We keep the Leader of the Opposition informed on the same national security matters on which we brief the Prime Minister, with some exceptions. The Director-General of Security also briefs leaders of political parties on any national security matters relevant to their party, such as foreign interference.

Responsibilities to other Ministers

240. Our statutory functions mean the Minister for Trade and the Minister for Communications may become involved in decisions made in accordance with the Telecommunications (Interception Capability and Security) Act 2013 relating to network security risks.

241. We also support the Outer Space and High-altitude Activities Act 2017 regulatory regime, which has been overseen by the Minister for Economic Development.

Private Secretary

242. GCSB and NZSIS currently provide a Private Secretary to the Office of the Minister Responsible for the GCSB and the NZSIS. Given the importance of this role, we ensure this person is an experienced staff member with knowledge and experience of our agencies. This arrangement means that you and your staff have an immediate source of advice and contact into our agencies. It also streamlines some of the security arrangements associated with handling highly classified material. We recommend this arrangement continue.

Strategic Direction Directorate

243. The Strategic Direction Directorate (SD) is responsible for providing day-to-day service to staff in your Office, and is led by Kate Pullar. SD will work with your office to establish your expectations about the frequency and nature of reporting we provide you, the management of Official Information Act 1982 and Privacy Act 2020 requests, and oral and written Parliamentary questions.