2.1. Overview of Key Agencies

Objective

2.1.1. Agency security personnel and senior management are aware of and utilise information security services offered by the New Zealand Government.

Context

Scope

2.1.2. This section provides an overview of the GCSB and other government organisations providing information security advice to agencies.

Government Communications Security Bureau

2.1.3. The Government Communications Security Bureau (GCSB) has two statutory missions: intelligence, and cyber security.

2.1.4. **Intelligence mission**

The GCSB uses signals intelligence collection capabilities to produce intelligence that provides decision advantage to government agencies in conduct of their legislatively mandated functions. The provision of this intelligence is one way that the GCSB contributes to the safety and security of New Zealand and New Zealand's interests.

2.1.5. **Cyber security mission**

New Zealand needs cyber security to:

- protect and maintain the digital services that the country relies on;
- protect its intellectual property;
- maintain its reputation as a stable and secure place to do business; and
- ensure that governmental and democratic processes remain free from interference.

2.1.6. The National Cyber Security Centre (NCSC) supports the GCSB's cyber security mission, including the Director-General's system leadership and GCISO responsibilities.

National Cyber Security Centre

2.1.7. As the Government's lead operational cyber security agency, the NCSC performs a range of functions, offers services, and supports New Zealand government agencies undertake their cyber security responsibilities.

2.1.8. The NCSC responds to cyber incidents that potentially affect New Zealand's security or economic wellbeing. It provides advanced cyber security services and advice to government agencies and nationally significant organisations to help defend them against cyber threats.

2.1.9. On 31 August 2023 CERT NZ was transferred to the NCSC to create a single operational cyber security agency.

2.1.10. The combined agency engages across the economy to improve the nation's cyber resilience. Supporting nationally significant organisations, businesses, organisations, and individuals who are, or may be, affected by cyber security incidents.

2.1.11. Agencies can contact the NCSC for advice and assistance on the reporting and management of information security incidents. The NCSC's response will be commensurate with the nature and urgency of the information security incident (see Section 7.2 – Reporting information security incidents). There is a 24 hour, seven day a week service available if necessary, by emailing ncscincidents@ncsc.govt.nz.

2.1.12. The NCSC provides specialist advice and assistance to New Zealand government departments in relation to cryptography, communications, and various information processing technologies.

2.1.13. The NCSC publishes the NZISM which sets out the information security requirements for New Zealand government organisations. An agency can contact the NCSC for advice and assistance relating to the interpretation of the NZISM by emailing: nzism@ncsc.govt.nz.

2.1.14. The NCSC supports regulatory regimes by providing risk assessments and advice to identify and manage risks to New Zealand's national security. Network operators can contact the Regulatory Unit by email: ticsa@ncsc.govt.nz.

2.1.15. The NCSC provides specialised technical security services focussed on countering unauthorised surveillance techniques and emanation security services focussed on preventing spread of unintentional signals. Contact the technical security services team by email: techliaison@gcsb.govt.nz.

2.1.16. Finally, agencies can contact the NCSC for advice and assistance on the purchasing, provision, deployment, operation, and disposal of High Assurance Cryptographic Equipment. The cryptographic liaison can be contacted by email at cryptohelpdesk@gcsb.govt.nz.

2.1.17. For general enquiries the NCSC can be contacted on info@ncsc.govt.nz.

Government Chief Information Security Officer

2.1.18. The Government Chief Information Security Officer (GCISO) is responsible for the strategic direction and prioritisation of the New Zealand Government's approach to information security and offers services to protect the Government's most sensitive information.

2.1.19. The role was created in response to the ongoing evolution of the cyber threat environment, emerging vulnerabilities, and technological change for the New Zealand Government.

2.1.20. The GCISO role was established by the Te Kawa Mataaho Public Service Commission in 2018. In July 2022, the Public Service Commissioner formally appointed the GCISO as System Lead for Information Security.

2.1.21. The GCSB Director-General holds the role of GCISO.

2.1.22. The GCISO draws on the technical expertise, relationships, and unique insights of both the NCSC and the GCSB to uplift information security practice across government.

2.1.23. The objective of the GCISO is to uplift cyber resilience in the Public Service, and enable secure digital transformation through specific initiatives, which focus on:

- promoting standards and policy.
- providing guidance.
- promoting secure by design.
- technical advice.
- increasing service delivery.
- building assurance; and
- supporting the information security workforce.

2.1.24. The NZISM is a key part of the GCISO's standards setting role. It is developed by the NCSC as part of its support of the GCISO.

2.1.25. The GCISO coordinates its system leadership role with other Te Kawa Mataaho Public Service Commission appointed system leaders, particularly the Government Chief Digital Officer (GCDO) and the Government Chief Data Steward (GCDS).

Government System Leadership

2.1.26. **Government Chief Digital Officer**

The GCDO is the government system lead for digital. This role oversees the development and management of digital for the state sector.

2.1.27. The GCDO is responsible for:

- setting digital policy and standards,
- improving investments,
- establishing and managing services,
- developing capability, and
- system assurance (assuring digital government outcomes).

2.1.28. **Government Chief Data Steward**

The GCDS is the government system lead for data. This role supports the use of data as a resource across government to help deliver better services to New Zealanders.

2.1.29. The GCDS responds to new and emerging data issues, and ensures that government agencies have the capability and skills to maximise the value of data. This is achieved through setting data standards, establishing common capabilities, developing data policy, strategy, and planning.

2.1.30. **Government Protective Security Lead**

The Government Protective Security Lead (GPSL) is the functional lead for protective security.

2.1.31. The GPSL provides the formal, system-level, functional leadership for government protective security.

2.1.32. **Government Chief Privacy Officer**

The Government Chief Privacy Officer (GCPO) is the government practice lead for privacy. This role leads an all-of-government approach to privacy to raise public sector privacy maturity and capability.

2.1.33. The GCPO is responsible for:

- providing leadership by setting the vision for privacy across government,
- building capability by supporting agencies to lift their capability to meet their privacy responsibilities,
- providing assurance on public sector privacy performance, and
- engaging with the Office of the Privacy Commissioner and New Zealanders about privacy.

2.1.34. **Government Procurement Lead**

The Government Procurement Lead is responsible for strengthening leadership and oversight of suppliers and agencies in key procurement sectors. A core part of this role is helping to ensure that agencies collaborate around sourcing and purchasing common goods and services. New Zealand Government Procurement and Property supports the Chief Executive of MBIE in their role as Procurement system lead.

2.1.35. Procurement system leadership works towards a procurement system that delivers better value for New Zealand and helps people, communities and businesses to thrive. This includes redesigning and repositioning the government procurement system to:

- make it easy for government agencies and suppliers to work together.
- lift procurement capability.
- improve the visibility of procurement activities and system performance; and
- facilitate and coordinate cross-agency collaboration.

Other government organisations

2.1.36. Archives NZ Te Rua Mahara o te Kāwanatanga

Archives NZ is the regulator of information created by the public sector, and reports to Cabinet on the state of Government recordkeeping.

2.1.37. Controller and Auditor-General Tumuaki o te Mana Arotake

The Controller and Auditor-General has two business units, the Office of the Auditor-General, and Audit NZ. Together they give Parliament and the public an independent view of how public organisations are operating.

2.1.38. Department of Internal Affairs Te Tari Taiwhenua

The Department of Internal Affairs has a range of relevant functions, including digital identity and digital safety, and regulatory functions including spam prevention and messaging compliance and money laundering. DIA provides guidance to support government organisations to use generative AI, cloud, enterprise architecture, government domain names, and APIs.

2.1.39. Department of the Prime Minister and Cabinet Te Tari o te Pirimia me te Komiti Matua

The Department of the Prime Minister and Cabinet's purpose is to advance an ambitious, resilient, and well-governed New Zealand. The National Security Group business unit provides leadership across New Zealand's national security community towards a secure and resilient Aotearoa New Zealand. The DPMC works on the Christchurch Call, critical infrastructure, and the National Security Intelligence Priorities.

2.1.40. Ministry of Business, Innovation & Employment Hīkina Whakatutuki

The MBIE works to ensure that telecommunications markets operate efficiently, and the commerce and ICT infrastructure is well developed. It is responsible for maintaining a robust regulatory environment for the ICT sector, and works to improve broadband and mobile connectivity for New Zealanders.

2.1.41.

Ministry of Foreign Affairs and Trade Manatū Aorere

MFAT ensures that New Zealander's can live, do business, travel and communicate more safely at home and offshore.

2.1.42. New Zealand Police Ngā Pirihimana o Aotearoa

The Police can investigate cybercrime and harmful digital communications.

2.1.43. New Zealand Security Intelligence Service Te Pā Whakamarumaru

NZSIS' mission is to keep NZ and New Zealanders safe and secure. The Director-General is the Government Protective Security Lead, and the NZSIS manages the Protective Security Requirements framework and maintains the Information Security Classification System.

2.1.44. Office of the Privacy Commissioner Te Mana Mātāpono Matatapu

The Office of the Privacy Commissioner works to develop and promote a culture in which personal information is protected and respected.

2.1.45. Public Services Commission Te Kawa Mataaho

The Public Services Commission monitors Public Service organisations and Chief Executives' performance.

References

2.1.46. The following websites can be used to obtain additional information about the security of government systems:

Organisation	Source
Archives New Zealand	https://archives.govt.nz
Audit New Zealand	https://auditnz.parliament.nz/
Office of the Auditor-General	https://oag.parliament.nz/
Department of Internal Affairs	https://dia.govt.nz https://digital.govt.nz
Department of Prime Minister and Cabinet	https://dpmc.govt.nz
Government Communications Security Bureau	https://gcsb.govt.nz
Ministry of Business, Innovation & Employment	https://mbie.govt.nz
Ministry of Foreign Affairs and Trade	https://mfat.govt.nz
National Cyber Security Centre	https://ncsc.govt.nz
New Zealand Security Intelligence Service	https://nzsis.govt.nz
New Zealand Police	https://police.govt.nz
Privacy Commissioner	https://privacy.org.nz
Protective Security Requirements	https://protectivesecurity.govt.nz
Public Service Commission	https://publicservice.govt.nz

Rationale & Controls

Organisations providing information security services

2.1.47.R.01. **Rationale**

If security personnel and senior management are not aware of the role government organisations play with regards to information security they

could be missing out on valuable insight and assistance in developing an effective information security posture for their agency.

2.1.47.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:199]**

Security personnel MUST familiarise themselves with the information security roles and services provided by New Zealand Government organisations.