



Briefing to the Incoming Minister for the Digital Economy and Communications

Date	31/01/2023
Priority	Routine
Security classification	RESTRICTED

Introduction

Welcome to your role as Minister for the Digital Economy and Communications. Part of your portfolio includes responsibility for cyber security policy. This responsibility is allocated by the Prime Minister from the National Security and Intelligence portfolio.

This briefing sets out:

- context of the portfolio, your roles and responsibilities, and how we can support you;
- key areas of focus requiring early consideration or decisions (in the first 100 days); and
- a selection of the longer-term priorities for the portfolio.

Cyber security policy is part of the Digital Economy and Communications portfolio, as cyber security is a key consideration in how the digital economy develops and the extent to which digital technologies are trusted. It therefore has significant implications for New Zealand's prosperity and New Zealanders' wellbeing. Opportunities to enhance New Zealand's security and resilience against cyber threats is a priority, given the impact that malicious cyber activity can have on our national security.

We look forward to supporting you to advance a secure, resilient, and prosperous online New Zealand.

Glossary

Acronyms commonly used in your portfolio include

CSSCC	Cyber Security Strategy Coordination Committee
DEC	Digital Economy and Communications
DPMC	The Department of the Prime Minister and Cabinet
GCSB	Government Communications Security Bureau
NCPO	National Cyber Policy Office
NCSC	National Cyber Security Centre
NSG	National Security Group
NSI	National Security and Intelligence
NSPD	National Security Policy Directorate
ODESC	Officials' Committee for Domestic and External Security Coordination

Your roles and responsibilities

Policy responsibility

The Minister for National Security and Intelligence has overall responsibility for national security policy. This portfolio includes cyber security policy, which has been allocated to you.

This includes:

- oversight, ongoing development and coordination of New Zealand's Cyber Security Strategy and associated work programme; and
- policy development related to:
 - the cyber resilience of New Zealand citizens, businesses, and critical infrastructure providers;
 - the national security implications of digital technologies including new and emerging technologies and applications of technologies;
 - growing the size and capability of the cyber security workforce in New Zealand;
 - incentivising the growth of the cyber security industry in New Zealand;
 - policy responses to cyber security incidents, including publicly attributing incidents in consultation with the Minister responsible for the Government Communications Security Bureau and the Minister of Foreign Affairs;
 - the national security implications of cybercrime; and
 - New Zealand's international engagement on cyber security policy issues, in consultation with the Minister of Foreign Affairs.

Statutory decision making powers

There are no specific statutory decision-making powers that sit within your allocated role for cyber security policy. You hold responsibility for the Cyber Security appropriation within Vote Prime Minister and Cabinet and therefore must meet the general duties and responsibilities of an appropriation Minister.

Related Ministerial portfolios

Cyber security is a cross-cutting issue impacting a number of portfolios. You will therefore have close engagement with a range of Ministers. In particular, you will work closely with the:

- Minister for National Security and Intelligence (the Prime Minister holds this Ministerial appointment);
- Minister responsible for the Government Communications Security Bureau (GCSB);

- Minister of Foreign Affairs.
- Minister of Justice; and
- Minister of Police;

Other Ministers you will interact with on a regular basis include:

- Minister of Defence;
- Minister for Economic and Regional Development
- Minister of Education
- Minister of Internal Affairs;
- Minister responsible for the New Zealand Security Intelligence Service (NZSIS); and
- Minister for Small Business.

Further information on Ministerial and government agency roles is included below and at Annex A.

Strategic context

Sector overview

Cyber security¹ is fundamental to New Zealand's national security and economic growth. Digital technologies have permeated almost every facet of economy and society, offering significant opportunities for innovation, stronger productivity, and improved services. COVID-19 accelerated the uptake of digital technologies and highlighted how they can increase resilience, enhance business and government operations, and enable education and social connections.

Along with these benefits come new challenges, including heightened exposure to cyber threats and attacks. Malicious cyber actors present a persistent threat to all New Zealanders and New Zealand organisations, businesses, and government. The impacts of cyber attacks can range from financial harm to an individual; loss of intellectual property and crucial data; loss of control of culturally important data; through to wide parts of society being denied access to critical services. Protecting the confidentiality, integrity, and availability of data systems, and networks is therefore fundamental.

Cyber security threats continue to grow in number, sophistication and complexity. This is being fuelled by a growth in the Internet of Things, and emerging technologies, such as 5G, artificial intelligence, and quantum computing. At the same time, malicious cyber actors globally – both state and non-state – are increasingly bold, sophisticated, and disruptive. Our international partners have intensified their efforts in response to these trends.

Cyber security is not a 'problem' that government can fix on its own. The bulk of cyber security capability and efforts exist outside government with individuals and private organisations working to protect their data and networked devices and infrastructure. Therefore, cyber security solutions require a multi-stakeholder approach, including the private sector, educational institutions, and civil society.

The government nevertheless has a leadership role to play in keeping New Zealand safe. This includes maintaining strong cyber security over our own networks, providing protection to citizens from serious cyber threats that no individual or organisation can mitigate on its own, and informing and promoting cyber security best practices to ensure individuals and organisations are getting the basics right to protect themselves. Government also works closely with international partners (both state and non-government) on various cyber security initiatives ranging from cooperation on cross-border cybercrime through to multilateral cooperation to promote a free open and secure internet.

Our core message to you is that cyber security is critical to ensuring New Zealand can realise the benefits of connectivity and digital innovation. In the face of increasing cybercrime and malicious cyber activity, we have an ambitious programme of work to enhance New Zealand's resilience against these threats. We are keen to focus this work to deliver on your priorities, and to sequence policy work and consultation on key areas carefully to ensure public and industry buy-in to deliver more effective cyber outcomes.

¹ "Cyber security" means protecting people and their computers, networks, programs, and data from unauthorised access, disruption, exploitation, or modification.

Cyber Security Strategy

New Zealand's approach to cyber security is set out in the Cyber Security Strategy. The most recent Cyber Security Strategy was released in 2019. Its vision is that "New Zealand is confident and secure in the digital world", and it outlines the areas in which we will prioritise action and investment. The Strategy takes an all-of-New Zealand approach to cyber security, in recognition that cyber risks are pervasive and, although the government has a significant role to play, it cannot address these risks alone.

There are five priority areas in the Strategy, each focused on improving different aspects of New Zealand's cyber security. The priorities are:

1. Cyber security aware and active citizens;
2. Strong and capable cyber security workforce and ecosystem;
3. Internationally active;
4. Resilient and responsive New Zealand; and
5. Proactively tackle cybercrime.

Budget 2019 allocated \$2 million per year to implement the Strategy.² This funding is used for joint-agency projects to enhance national cyber security and lift cyber resilience at a system level, in areas that are not well addressed by other forms of government expenditure. DPMC is the appropriation administrator. The inter-agency Cyber Security Strategy Coordination Committee (CSSCC) is responsible for allocation and oversight of the Strategy funding and work programme.

Since the launch of the Strategy in 2019, Government has undertaken a range of projects and initiatives to influence the cyber security environment and enhance New Zealand's cyber security capability, under the five priority areas. Projects supported to date have included:

- Establishment of a temporary Cyber Security Advisory Committee which provided executive-level, industry-centric advice on options for strengthening New Zealand's cyber security and resilience (complete)
- Research on the domestic cyber security workforce and skills ecosystem, covering size, roles demographics, pathways, and key skills gaps (complete)
- Translation of CERT NZ resources into Māori, New Zealand Sign Language, and other languages (in progress)

² This is additional to other cyber security funding across government. For instance, through Budget 2022, the Government committed over \$30 million of funding for CERT NZ to improve New Zealand's cyber resilience, alongside almost \$19 million for the GCSB's National Cyber Security Centre to maintain and improve its cyber security and information security services.

- A contribution to Cyber Skills Aotearoa, which is delivering resources in schools to support students to develop cyber security skills and gain awareness of career opportunities in this field (in progress)
- A contribution to the Global Conference on Cyber Capacity Building, which is seeking to enhance collaboration on and coordination of global cyber capacity building efforts (in progress)
- A National Cyber Security Exercise and business case to establish a national exercise capability (in progress)
- A National Cyber Security Risk Assessment to build understanding of the risks prevalent across the current cyber security threat landscape to inform future policy and investment advice (in progress)

Implementation of the Cyber Security Strategy also supports delivery of the Digital Strategy for Aotearoa, and particularly the theme Mahi Tika (Trust).

The Cyber Security Strategy 2019 focused on a five-year period, through to 2023. s9(2)(f)(iv)

Long-term insights

The current cyber threatscape in New Zealand

S 9(2)(g)(i)

Underreporting of cyber incidents is common, and the wider impact of significant events, including incidents that trigger a national security response, are often not adequately quantified. Data loss, from espionage or intellectual property theft, may occur without the victims' knowledge.

Public reporting to CERT NZ provides some insights into the growth and scale of the problem. In 2021, 8,831 incidents were reported to CERT NZ, a 13% increase on 2020. It is notable that the mix of reported incident changes year on year, reflecting the evolving nature of the threat.³ The NCSC recorded 350 incidents affecting nationally significant organisations in the 2021/22 year. Of the incidents recorded by the NCSC, 34% showed links to suspected state-sponsored actors.

Cyber attacks against New Zealand organisations will continue to increase in number, sophistication, and impact. However, New Zealand's experience is not unique – it reflects a serious and growing international problem.

Cyber threat trends

Current global cyber threat trends include:

³ 2021 Report Summary, CERT NZ

- An increase in the speed and scale of scanning and mass exploitation of recently disclosed vulnerabilities. Malicious actors are quickly taking advantage of vulnerabilities to establish a foothold into networks, and then selectively pick their targets for further compromise.
- Establishment of more strategic access, for example through the compromise of supply chains. The growing trend of outsourcing technology services can expose enterprises to increased risk as recent compromises, s9(2)(f)(iv)
- Private actors selling increasingly sophisticated cyber tools, including greater use of ransomware and malware 'as a service' that reduce technical barriers to entry. The ransomware ecosystem has been commoditised, enabling complex and impactful campaigns to be carried out by malicious actors with a much lower technical skill base.
- The growing use of cyber tools by state cyber actors to pursue geopolitical advantage. This might be aimed at strengthening influence, stealing commercially valuable information, undermining or embarrassing other states, creating chaos and disruption, retaliating for the actions of other states, or pre-positioning for future advantage.
- The blurring of the lines between state-sponsored and criminally motivated actors. For example, criminal actors are using capabilities that recently were mainly in the hands of sophisticated state actors. Similarly, some cyber criminal groups are provided 'safe havens' by their resident countries from which they can operate without sanction.

All this contributes to making the global cyber threat picture more complex, effective cyber security measures more challenging to implement, and attribution of cyber incidents to particular actors more difficult.

Areas of opportunity

In this context, there is an opportunity for New Zealand to enhance its resilience to cyber threats, both existing and emerging, to support our future prosperity and wellbeing. This includes a number of areas in which government can play a leading role:

- supporting individuals and organisations of all sizes to understand and prevent the threats themselves;
- preventing the most significant attacks against our critical infrastructure and organisations – or deterring and disrupting cyber activities to mitigate the impacts of threats;
- identifying and mitigating vulnerabilities to build collective resilience and ensure that we are able to respond and recover when subject to attack; and
- collaborating with partners both domestic and international, government and non-government, in support of these components.

The strategic work programme led by NCPO seeks to deliver progress on these areas, aligned with the five priority areas of the Cyber Security Strategy. s9(2)(f)(iv)

s9(2)(f)(iv)

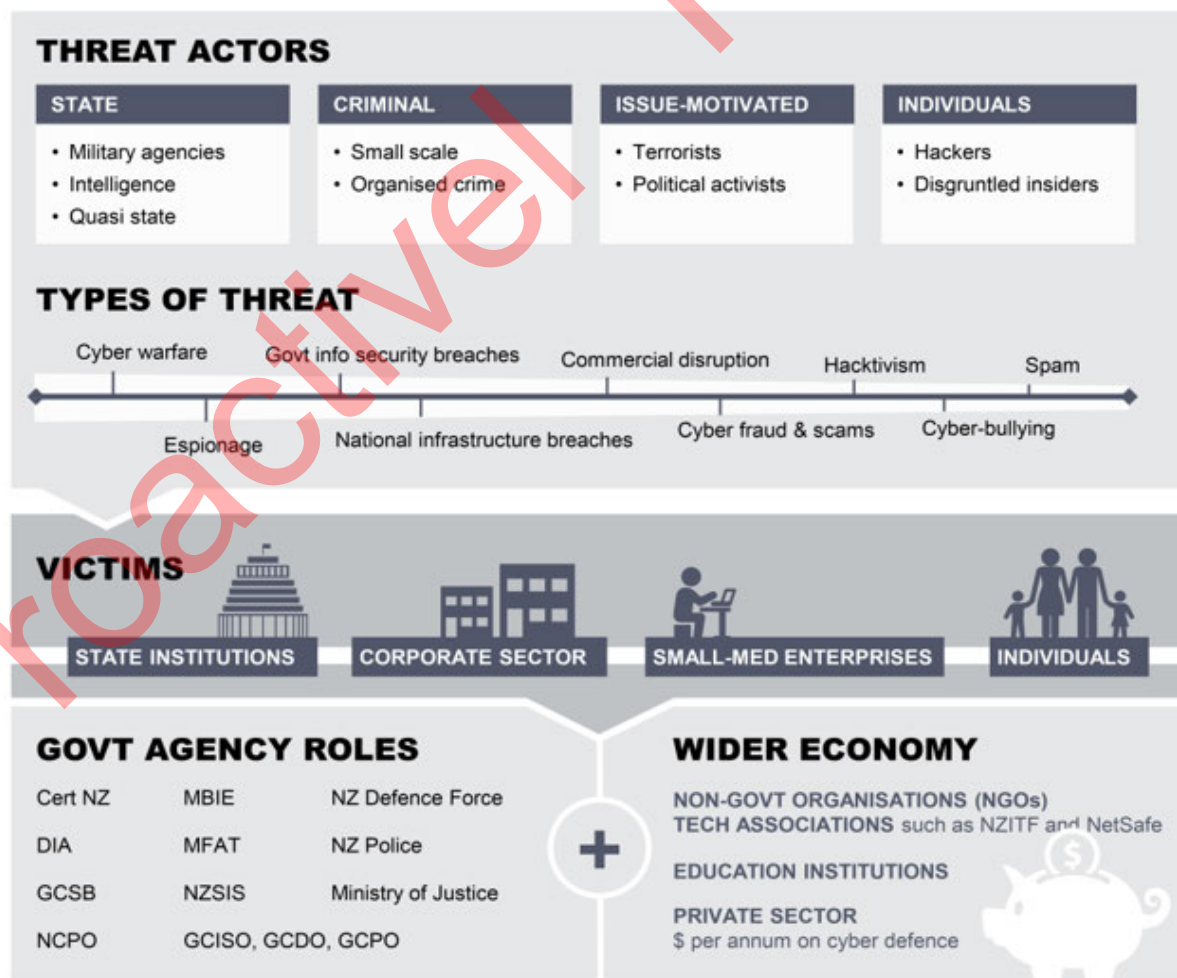
Key areas of focus and priority initiatives are outlined under the “immediate priorities” and “longer-term priorities” sections below.

A further area of opportunity is the development of New Zealand’s first National Security Strategy, which DPMC is leading as part of the Government’s response to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019. The National Security Strategy will ensure that our national security agencies contribute to a thriving, secure, and resilient New Zealand, and that the interests of our communities and the nation are at the heart of what they do.

This Strategy will provide an overarching framework under which the Cyber Security Strategy and other sector-specific strategies will sit. s9(2)(f)(iv)

Key stakeholders

The diagram below provides a brief overview of the cyber security landscape.




Three Ministerial portfolios currently have direct policy responsibility for cyber security matters:

- The **Minister for National Security and Intelligence** has overarching responsibility for the national security and intelligence system and setting the overall policy for that system.
- The Minister for National Security and Intelligence has allocated responsibility for cyber security policy to the **Minister for the Digital Economy and Communications** (and, prior to that, to the Minister for Broadcasting, Communications and Digital Media).
- The **Minister for the Digital Economy and Communications** also has responsibility for CERT NZ.
- The **Minister responsible for the GCSB** has responsibility for the oversight of the GCSB and its cyber security functions, as set out in the Intelligence and Security Act 2017.


There are a number of agencies that do work which touches on the Ministerial portfolios. These are outlined at Annex A.

Immediate priorities and key areas of focus

s9(2)(f)(iv)

Four horizontal grey bars of varying lengths, representing redacted text.

s9(2)(f)(iv)

A large grey rectangular block covering the majority of the page content, indicating a full-page redaction. A large, diagonal, semi-transparent red watermark reading "Proactive! Released" is overlaid across the entire page.

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)() (iv)

s9 2)(f)(iv)

s9(2)(f)(iv)

~~RESTRICTED~~

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

~~RESTRICTED~~

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv) [REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]

s9(2)(f)(iv) [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
s9(2)(b)(i) [REDACTED], s9(2)(f)(iv) [REDACTED]
[REDACTED]
[REDACTED]

s9(2)(f)(iv) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

s9(2)(f)(iv)

s9(2)(f)(iv)

Accession to the Budapest Convention

New Zealand is in the process of **acceding to the Council of Europe Convention on Cybercrime (known as the Budapest Convention)**. The Convention addresses cross-border cybercrime by harmonising national laws, and improving investigative techniques and cooperation among nations. New Zealand already complies with most of the requirements of the Convention, but in order to accede, would need to adopt additional measures enabling law enforcement agencies to order preservation of computer data to support cooperation on international investigations. A Bill is expected to be introduced to Parliament by April 2023 which introduces a data preservation regime, and makes several other minor procedural changes. This work is led by the Minister of Justice, supported by you. Accession to the Budapest Convention is crucial to our efforts to counter cybercrime s9(2)(f)(iv)

In parallel, at Cabinet's direction, officials in the NCPO and Ministry of Justice are working to establish a mechanism for the government to **engage with Māori stakeholders** on the implications for Māori of acceding to the Budapest Convention, and to authentically integrate te ao Māori into the development of policy proposals for any other future cross-border data access agreements.

This work contributes to three of the five priority areas of the Strategy: internationally active; resilient and responsive New Zealand; and proactively tackling cybercrime.

Upcoming decisions

s9(2)(f)(iv)

Longer-term priorities

This section describes a selection of the future and longer-term priorities on which we will update you and seek your input in slower time. There are further areas of policy work and international engagement, including opportunities for you to engage with international partners, on which we will brief you in future.

International collaboration on ransomware

In 2021, New Zealand joined the U.S.-led Counter Ransomware Initiative (CRI). The platform, comprising 36 countries and the EU, promotes closer international cooperation in efforts to strengthen resilience and combat ransomware. s6(a)

Public safety and law enforcement in a digital age

As technology is evolving, ensuring effective public safety and law enforcement is becoming more difficult. There are several areas of work that seek to consider how we can balance the opportunities and advantages of digital technologies, with the needs of law enforcement and intelligence agencies.

Encryption

Encryption plays a crucial role in cyber security, protecting personal data, privacy, intellectual property, and trade secrets. In repressive states it is also important for protecting journalists and human rights defenders. Particular implementations of encryption technology can, however, pose challenges to law enforcement and public safety, including to highly vulnerable members of society.

As a growing number of technology platforms roll out end-to-end encryption, officials have commenced work to understand **the impact of end-to-end encryption on investigations and public safety in New Zealand**. The work will assess how law enforcement may be able to access the information it needs to protect individuals from harm, while protecting the rights of individuals to privacy and security, and applying the principles of the Treaty of Waitangi Te Tiriti o Waitangi. The work will explore solutions for proportionate, reasonable, and necessary law enforcement access and review whether agencies are taking full advantage of existing regulations and capabilities. This work will inform future advice to Ministers.

Complementary work is considering what public safety and law enforcement will look like due to the logical consequences of current trends or technologies that are on the horizon but not yet ubiquitous, and what policy options we might want to explore to mitigate potential risks.

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

S9(2)(f)(iv), S9(2)(b)(ii)

3(2)(f)(iv)

Our support for you

About DPMC

DPMC's purpose is to advance an ambitious, resilient, and well-governed New Zealand, and we do this in a wide variety of ways. We lead, advise, steward, and deliver activities across the public sector, and provide specific advice and support to the Governor-General, Prime Minister, and our portfolio Ministers. As one of the three central agencies, we also play a role in leading and coordinating public service agencies.

Ultimately, our work is about making sure we are working together effectively across the public sector to deliver on the Government's priorities and provide the services and outcomes New Zealanders need.

DPMC is uniquely placed within the public service, in terms of our whole-of-government perspective and our inherent closeness to Ministers.

Providing expert policy advice

One of the most important things in implementing your programme is ensuring that we provide strategic advice, working in collaboration with other agencies, industry, and non-government and international partners to ensure comprehensive, strategic, all-of-society policy and investment advice on cyber security.

The National Cyber Policy Office (NCPO)

Established in 2012, NCPO formally reports to you on cyber security policy matters, consulting with other Ministers as appropriate. NCPO leads the development of cyber security strategy and policy advice for the government and advises the government on its investment of resources in cyber security activities. This includes developing and coordinating implementation of cyber security strategies. NCPO oversees the implementation of the current New Zealand Cyber Security Strategy.

NCPO conducts international engagement (working with the Ministry of Foreign Affairs and Trade and others) and works closely with counterpart policy teams in Australia, Canada, the United Kingdom, the United States, and other like-minded countries.

NCPO, along with the Cyber Coordinator (see below), also conducts outreach with the private sector and civil society on cyber security policy issues.

NCPO is a team of approximately ten staff, sitting in the National Security Policy Directorate within DPMC's National Security Group and reporting to Tony Lynch as DPMC's Deputy Chief Executive, National Security. We would be happy to brief you on the work of the National Security Group.

DPMC provides a part-time Private Secretary to support your cyber security policy work.

Cyber Security Strategy Coordination Committee

The Deputy Chief Executive, National Security chairs an inter-agency Cyber Security Strategy Coordination Committee (CSSCC). This committee meets every two months, and is the key 'clearing house' to govern the annual work programme to implement the Strategy, track progress, ensures initiatives are aligned and any gaps identified, and assess the overall direction of New Zealand's cyber security ecosystem.

Committee members include representatives from DPMC; Crown Law; Department of Internal Affairs; Government Communications Security Bureau; Ministry of Business, Innovation and Employment; Ministry of Defence; Ministry of Foreign Affairs and Trade; Ministry of Justice; New Zealand Defence Force; and New Zealand Police.

PM's Special Representative on Cyber and Digital

The Prime Minister has a Special Representative on Cyber and Digital, who is based in the Policy Advisory Group of DPMC. The Special Representative primarily leads the delivery of the Christchurch Call with support from a small Christchurch Call Unit, which is currently funded from the Cyber Security Strategy appropriation, with one Christchurch Call workstream funded from the Prime Minister's Multi-Category appropriation.

The PM's Special Representative is also focused on senior-level engagement with the technology sector in New Zealand and overseas to address online and digital challenges, and plays a coordination role in specific areas. This includes supporting the development of onshore cloud computing capabilities, engagement with industry and international partners on encryption (alongside NCPO), and work with industry, civil society, and partners on various other digital and online issues. NCPO works closely with the PM's Special Representative and the Christchurch Call Unit on areas of mutual interest.

Funding and reporting is managed by DPMC

The Department of the Prime Minister and Cabinet administers all appropriations within Vote Prime Minister and Cabinet. Funding for DPMC's contribution to your portfolio sits within Vote Prime Minister and Cabinet's Cyber Security appropriation.

DPMC is responsible for coordinating the annual accountability process, responses for the Governance and Administration Select Committee hearings, and funding proposals.

As part of the Estimates of the Appropriations passed by Parliament, performance measures are attached to funding within your portfolio. This includes an annual Ministerial satisfaction survey which you will be required to complete, although we appreciate feedback at any time

Annex A

Government agencies involved in cyber security

- **DPMC**, through the National Security Group, leads advice on matters for national security for the: Prime Minister (who is the Minister for National Security and Intelligence); the Minister for the Digital Economy and Communications (on matters associated with cyber security policy through the NCPO); the Minister responsible for the New Zealand Security Intelligence Service; and the Minister responsible for the GCSB (in the context of the Intelligence and Security Act 2017). DPMC provides advice on the Intelligence and Security Act 2017. DPMC also leads on advice for the Five Country Ministerial meeting, most recently attended by the Minister of Justice which often includes cyber security related topics. DPMC is also the home agency of the PM's Special Representative on Cyber and Digital and the Christchurch Call Unit, reporting to the Prime Minister.
- The **Government Communications Security Bureau (GCSB)**, through the **National Cyber Security Centre (NCSC)**, provides cyber security services, including raising cyber resilience through threat reporting, advice, and guidance; incident response capabilities and support to major events; and the provision of detection and disruption services to consenting organisations. The focus of the NCSC is on nationally significant organisations, or where there is a risk of high national impact.
- The Director-General GCSB is the **Government Chief Information Security Officer (GCISO)** and is the functional lead for information security across government. Along with the GCISO functional leadership, the GCSB maintains the New Zealand Information Security Manual, which is a mandatory component of the Protective Security Requirements for agencies. The GCSB also has a regulatory function, administering the network security provisions of the Telecommunications (Interception Capability and Security) Act 2013.
- The **New Zealand Security Intelligence Service (NZSIS)** delivers the Protective Security Requirements, which includes information security, for government agencies.
- **New Zealand Police** is responsible for countering, investigating, and prosecuting cybercrime and cyber-enabled crime, including cyber aspects of transnational organised crime.
- The **Department of Internal Affairs (DIA)** Chief Executive is the Government Chief Digital Officer (GCDO). This digital functional/system role is responsible for implementing the Strategy for a Digital Public Service, with a focus on trusted digital government and using all of government contracts to build a more secure digital system. DIA also implements the Unsolicited Electronic Messages Act 2007 and the Films, Videos and Publications Classification Act 1993. The latter focusses on addressing online sexual exploitation of children, and violent extremism online.
- The **Ministry of Justice** works on the rule of law and justice sector policy, including oversight of the Harmful Digital Communications Act 2015 and the Privacy Act 1993, and the legal framework for lawful access to evidence, including electronic evidence.
- The **Ministry of Business, Innovation and Employment (MBIE)** has links with cyber security in the areas of communications policy, the Digital Economy Work Programme

~~RESTRICTED~~

including the Digital Strategy and Digital Technologies Industry Transformation Plan, research and innovation, consumer advice, and support for small businesses. MBIE advises the Minister for the Digital Economy and Communications (you) on the Telecommunications (Interception Capability and Security) Act 2013, which sets out the obligations of the communications industry in relation to legal interception and network security, and the Unsolicited Electronic Messages Act 2007.

- **CERT NZ** receives reports of cyber incidents, analyses threats, shares information and advice, coordinates incident responses, provides cyber capacity-building in the Pacific, and is a point of contact for the international CERT community. CERT NZ is a branded business unit within MBIE.
- The **Ministry of Foreign Affairs and Trade** works jointly with NCPO on cyber security diplomacy, including cyber security dialogues with other countries, capacity building in the Pacific, advancing norms of state behaviour online, coordination among partners of public attribution statements, and addressing barriers to trade arising from other countries' cyber security regulations.
- The **Ministry of Defence** and the **New Zealand Defence Force** (NZDF) are focused on the cyber protection of the NZDF networks and deployed operations, as well as the long-term structure for raising, training, and sustaining cyber capabilities.