Department of the Prime Minister and Cabinet

National Cyber Policy Office Proactive Release
April 2018

The document below is released by the Department of the Prime Minister and Cabinet relating to the refresh of New Zealand's Cyber Security Strategy and Action Plan.

Some parts of this document 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.

Date: March 2018

Title: Refresh of New Zealand's Cyber Security Strategy and Action Plan (to Cabinet External Relations and Security Committee).

Information withheld with relevant section(s) of the Act:

Paragraph 16, bullet point 4
s 6(a) – security or defence of New Zealand.
s 6(c) – maintenance of the law

Paragraph 17, bullet point 1, sentences from paragraphs 23, 31, 55, Recommendation 8.4, sentence from Appendix two bullet point 10
s 6(a) – security or defence of New Zealand.

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

27 March 2018

Chair
Cabinet External Relations and Security Committee

REFRESH OF NEW ZEALAND'S CYBER SECURITY STRATEGY AND ACTION PLAN

Proposal

1. This paper seeks agreement to a comprehensive refresh of New Zealand's Cyber Security Strategy and Action Plan.

Executive Summary

2. There has been good progress to improve New Zealand's cyber security under the Cyber Security Strategy and Action Plan approved by Cabinet in 2015.

3. This includes establishment of CERT NZ, delivery of CORTEX malware detection and disruption services, cyber security awareness campaigns, the first Cyber Security Summit, Protective Security Requirements for government agencies, work to improve the cyber security of small businesses, a focus on building a cyber security workforce, developing NZ Police skills to respond to cybercrime and international engagement on cyber security issues.

4. This Government has committed to building a connected nation, promoting and protecting digital rights, and harnessing digital technology for economic growth, community benefit and innovation. Cyber security is essential to this.

5. There is an upwards trajectory of cyber security threats. The widespread use of connected devices and emerging technologies has expanded the attack surface for malicious threat actors. Both CERT NZ and the National Cyber Security Centre (within the Government Communications Security Bureau) have reported a growing number of incidents. Globally, it is clear that cyber threat actors are increasingly bold, brazen and disruptive. Our international partners have intensified their efforts in response to this problem.

6. It is timely for New Zealand to step up its cyber security efforts. This would complement other initiatives underway, such as the development of a Digital

Strategy for New Zealand, the proposed establishment of a Chief Technology Officer and the priority accorded to digital rights.

7. A refresh of the Cyber Security Strategy and Action Plan will involve a broad range of agencies, consultation with the private sector and non-government organisations, and analysis of international best practice. Draft Terms of Reference have been developed.

8. The refresh will analyse gaps and opportunities to improve New Zealand's cyber security. It will assess institutional arrangements for cyber security, collaboration with the private sector, efforts to address cybercrime, system-wide leadership of government information security, international cyber cooperation and responses, opportunities to grow the cyber security sector, and the security challenges of emerging technology.

9. It will result in recommendations for a new Cyber Security Strategy and Action Plan.

Background

10. In November 2015, Cabinet approved New Zealand's second Cyber Security Strategy, Action Plan and National Plan to Address Cybercrime [NSC-15-Min-0012].

11. The Strategy has served us well as an overarching framework for cross-government work under four goals (cyber resilience, cyber capability, addressing cybercrime, and international cooperation).

12. The ITU's Global Cyber Security Index for 2017 ranks New Zealand in the top group of 21 leading countries. The Australian Strategic Policy Institute's cyber maturity index for 2017 ranked New Zealand as sixth for the Asia Pacific region, behind the United States, Australia, Japan, Singapore and Republic of Korea.

Good progress has been made to implement the 2015 Cyber Security Strategy and Action Plan

13. Good progress has been made under each of the four goals of the Strategy.

14. Under the **Cyber Resilience** Goal, progress includes:

- CERT NZ was established in April 2017 to receive reports of cyber incidents, analyse threats, share information and advice, coordinate incident responses and be an international point of contact.

- The Government Communications Security Bureau's National Cyber Security Centre (NCSC) delivered its three-year long CORTEX capability development project. These capabilities enable the NCSC to analyse, detect and disrupt cyber threats against public and private sector organisations. Through the insights it gleans from CORTEX capabilities, the NCSC is also able to provide cyber security advice and guidance to hundreds of organisations of national significance.

- Following on from the successful completion of project CORTEX and the Malware-Free Networks pilot – which involved collaboration with private sector partners – the NCSC will be submitting recommendations to Cabinet in March 2018, regarding the future form of the Malware-Free Networks capability.

- The New Zealand Defence Force is developing a cyber security and support capability to ensure it is prepared to defend its networks at home and its operations abroad.

- The Cyber Security Emergency Response Plan is tested through exercises and used to guide incident response.

15. Under the **Cyber Capability** Goal, progress includes:

- With modest funding, the government has supported annual cyber security awareness campaigns, developing practical resources to assist individuals, businesses and organisations to build their cyber security capability.

- The first Cyber Security Summit was held in May 2016 with the aim of embedding cyber security at the business executive and governance levels.

- The government's Protective Security Requirements have enabled agencies to assess and improve their information security.

- A "cyber credentials" scheme to help small businesses access practical and affordable cyber security support has been developed and will be delivered by private sector providers.

- A Cyber Security Skills Taskforce has focused on practical initiatives to help build a cyber security professional workforce, including the establishment of a level six cyber security qualification.

16. Under the **Addressing Cybercrime** Goal, progress includes:

- A National Plan to address Cybercrime was released as part of the 2015 Strategy – but progress has been limited by resources and competing priorities.

- NZ Police's "National Cybercrime Operating Strategy" focuses on prevention.

- Specific training courses have been developed to improve the ability of District police officers to respond to cybercrime.

- s6(a) [redacted] s6(c) [redacted]

17. Under the **International Cooperation** Goal, progress includes:

- s6(a) .

- There has been particularly close trans-Tasman cyber cooperation, with areas highlighted annually in the Prime Ministers' Joint Statements.

- New Zealand has held two cyber dialogues with China and one each with India and Singapore. There have also been useful cyber security discussions with Israel, the Netherlands and Japan.

- Regional cyber security is pursued through the ASEAN Regional Forum and the ASEAN Defence Ministers Meeting (Plus).

Why is a new Cyber Security Strategy and Action Plan needed?

Cyber security is an essential element of a connected, digital nation

18. This Government has committed to building a connected nation and harnessing digital technology for economic growth, community benefit and innovation. I intend to develop a Digital Strategy for New Zealand which will reflect a joined up response by government to digital technologies.

19. This includes the promotion and protection of digital rights. A secure cyberspace is integral to digital rights, enabling New Zealanders, businesses and organisations to have trust and confidence in the integrity and privacy of their online information.

20. As we embrace digital technology, however, it is apparent that this same technology has provided new avenues for criminals and hostile actors to gain advantage. The widespread use of connected devices and emerging technologies has expanded the attack surface for malicious threat actors.

21. Cyber security is therefore essential to ensure that the gains of digital technology are not eroded, to protect the information and networked systems that are vital to our economic growth, and to enable New Zealanders to interact online without suffering harm.

There are increasing cyber security threats

22. The clear trend is an upward trajectory of cyber security threats. Cyber threat actors are increasingly bold, brazen and disruptive. New Zealand's geographical location does not exempt us from this threat.

23. Over the last year, New Zealand has recorded an increased level of cyber threats, including the New Zealand implications s6(a) the WannaCry ransomware (May 2017) and the notPetya ransomware (June 2017).

24. The National Cyber Security Centre (within the Government Communications Security Bureau), which focuses on countering sophisticated cyber threats and protecting New Zealand's networks of national importance, recorded 396 incidents over the 2016-17 year, including providing hands-on intensive incident response on 31 occasions[1].

25. The nature of the threat is illustrated by case studies in the NCSC's annual threat report. An example is the compromise of a New Zealand organisation's network by a state sponsored threat actor which then used the network to mount a cyber attack on a foreign organisation.

26. In its latest quarterly report (July – September 2017), CERT NZ received 390 incident reports – with 43% from businesses and organisations. This involved losses of $1.1 million, with 29% of those people who reported to the CERT experiencing financial loss.

27. Globally, notable examples include the reports of Russian interference in the United States 2016 elections; the theft of 21 million personnel details from the United States Office of Personnel Management (attributed in the media to Chinese espionage) and cybercrime data breaches such as the revelation in October 2017 that 3 billion Yahoo user accounts had been breached in 2013.

28. Accordingly, New Zealand must increase the momentum of its cyber security efforts to manage the cyber security risk and keep pace with this threat trajectory.

Our international partners have intensified their cyber security efforts.

29. The United Kingdom released an ambitious £1.9 billion Cyber Security Strategy in November 2016, (its third Strategy in seven years), aimed at defending the UK, deterring and disrupting hostile action, developing an innovative cyber industry and talent pipeline, and international action to shape approaches to cyberspace.

30. Australia's 2016 Strategy is now accompanied by a comprehensive international cyber engagement strategy released in October 2017. The latter emphasises the value of an open, free and secure cyberspace, aims to harness the opportunities of the digital age and is clear about action to deter unacceptable behaviour in cyberspace.

31. Canada is about to announce its new Strategy. s6(a) [redacted] Singapore, basing its Strategy on New Zealand's model, is investing heavily in cyber defences.

32. It is appropriate to examine whether New Zealand is making an appropriate contribution, alongside our partners, to address the cyber security challenge.

[1] National Cyber Security Centre, "Cyber Threat Report 2016-17", 22 November 2017: https://www.ncsc.govt.nz/newsroom/2016-17/

Demonstrating the government's commitment to cyber security

33. The government is committed to ensuring the integrity and efficacy of our electronic, communications, and digital infrastructure. The aim is to ensure New Zealanders have confidence in cutting edge security that protects their communications, intellectual property and online footprint. As more systems are networked and connected to the Internet, it is imperative that they are protected from cyber threats, both criminal and state-sponsored.

34. To achieve this commitment, I recommend a comprehensive refresh of the New Zealand Cyber Security Strategy and Action Plan is carried out. This will be an opportunity to demonstrate the importance this Government attaches to cyber security as an integral component of the digital revolution, and provide certainty about the Government's intentions in this area.

35. It would complement other initiatives already underway, such as the development of a Digital Strategy for New Zealand, the proposed establishment of a Chief Technology Officer and the priority accorded to digital rights.

36. A refresh of the Cyber Security Strategy and Action Plan would enable us to test whether we are investing the right resources and structuring our efforts, in the right way, across protective security, civilian, military, law enforcement, and intelligence agencies to make the greatest improvement to the security of our digital infrastructure and communications.

37. It is timely for New Zealand to step up its cyber security, so that we are not left vulnerable to cyber intrusions at the expense of our security and economy – and so that we can fully achieve the benefits of a connected nation.

How should we approach the cyber security refresh?

38. A broad range of agencies contributes to New Zealand's cyber security. Cyber security is relevant to national security and intelligence, defence, international relations, trade, economic development and innovation, criminal justice, education, government digital transformation, and public service delivery. See Annex Two for an outline of the cyber security roles of the key government agencies.

39. The refresh of the Cyber Security Strategy and Action Plan will require collaboration across a number of Ministerial portfolios. I propose to work closely with all of the relevant Ministers as we determine the priorities and initiatives to be incorporated in a refreshed Cyber Security Strategy and Action Plan.

40. A successful refresh of the Cyber Security Strategy and Action Plan will involve hand-in-hand partnership with the private sector and non-government organisations to seek their views on "what more the government can do to improve New Zealand's cyber security". We have a collective responsibility to continue to ensure the needs of the corporate sector operating New Zealand's critical national infrastructure and networks are well supported; to tap into the cyber security expertise of ICT businesses; and engage with businesses and organisations vulnerable to cybercrime and harmful cyber intrusions.

41. Much can be learned from two-way engagement with like-minded and similar-sized countries. Estonia, the Netherlands, Israel and Singapore are particular exemplars (with Singapore drawing heavily on New Zealand's 2015 Strategy). Australia, the United Kingdom, and the Scandinavian countries have also developed sound and robust strategies for dealing with the cyber security challenge. We have strong contacts with counterparts in these countries and a track record of working with them and learning from each other on priorities and current approaches to cyber security.

42. Proposed Terms of Reference for the refresh of New Zealand's Cyber Security Strategy and Action Plan are attached at Annex One.

What should be covered by the cyber security refresh?

43. Officials have informed me of a number of areas that can contribute to an improved systemic approach to identifying, managing and reducing the consequences of cyber security risks.

<u>The complex cyber security landscape: partnership</u>

44. The current Strategy deliberately takes a broad approach to improving the cyber security of New Zealand, emphasising multiple actions rather than a single intervention. This reflects the range of threat actors and the variety of cyber threats which can affect government agencies, the corporate sector, small businesses and individuals. A broad range of agencies, in partnership with the private sector, is required to contribute to New Zealand's cyber security.

45. The cyber security landscape is complex. In the national security context, it is recognised that risks have effects across the system, beyond the remit of any single agency. To achieve national resilience, agencies must contribute to a systemic approach to identifying and managing risks. Likewise, I consider that a systemic approach is essential for New Zealand to deal with the cyber security challenge.

46. Just as I have proposed with the Digital Strategy, I would like this refresh to consider ways to promote a more joined-up approach to cyber security by government agencies, in cooperation with the private sector and non-government organisations. The current Strategy emphasises, as one of its four principles, that partnerships are essential.

47. This refresh of the Cyber Security Strategy and Action Plan provides an opportunity to look at the cyber security roles of agencies. We need to continue assessing whether we have the optimal arrangements and resources for effectively addressing cyber security efforts across government. The State Services Commission will be closely involved if any machinery of government issues arise in this context.

48. In this regard, work is underway to improve the system-wide understanding and mitigation of cyber security risks to government agencies. We must ensure the integrity and security of our increasingly digitalised government services.

49. I would also like to explore innovative models to achieve strong cyber security collaboration between the government and the private sector and non-government organisations. A structured approach to ensuring private sector engagement with the government's work (and vice versa) might be one option for consideration. This could include considering models such as advisory boards or a cyber security council[2]. It may help us to get the right level of engagement with the private sector on cyber security – a challenge which our international partners also face.

Addressing Cybercrime

50. New Zealand has a National Plan to Address Cybercrime. Implementation has, to date, been modest. I expect this refresh of the Cyber Security Strategy and Action Plan to assess whether NZ Police and other agencies have sufficient resources and appropriately trained staff to protect New Zealanders from online crimes and deal with the challenges of emerging technologies.

51. The current Action Plan proposed that New Zealand's policy and legislative framework should be tested to see whether it remains fit for the purpose of dealing with cybercrime in the digital age. This action has yet to be completed. I propose this work should remain part of New Zealand's cyber security agenda.

52. Cybercrime is a transnational issue, with perpetrators operating across borders. International collaboration must continue to be part of the solution. I would like the refresh to explore whether NZ Police's existing international links are sufficient to deliver a comprehensive response to cybercrime. This could include exploring opportunities to build closer links with key international cybercrime units such as the European Cybercrime Centre within Europol and the International Cybercrime Coordination Cell with the Federal Bureau of Investigation.

53. The ability of New Zealand agencies to collaborate more effectively with international counterparts to address cybercrime would be assisted by accession to the Council of Europe Convention on Cybercrime (known as the Budapest Convention). Work is now underway - led by the National Cyber Policy Office and Ministry of Justice - to outline what measures might be required to bring New Zealand's laws and investigative processes in line with the Convention. Cabinet will consider whether New Zealand should formally express interest in accession to the Convention, and the steps towards accession.

Cyber diplomacy, deterrence and responses

54. I recommend that we expand our international cyber efforts. This is likely to require additional resources. In the face of increasingly brazen cyber actions, New Zealand will need to be seen and heard in global dialogue on norms of acceptable state behaviour in cyberspace, the applicability of international law, and the importance of an open, free and secure Internet.

[2] The National Cyber Security Framework Manual (an internationally recognised best practice guide for states on cyber security published by the NATO Cyber Cooperative Centre of Excellence in Tallinn, Estonia) emphasises the importance of "Whole of Nation" cooperation, referencing the example of the Dutch National Cyber Security Council. https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

55. We will need to consider the mechanisms available to us to dissuade or deter malicious cyber activities, particularly where it is state-sponsored or state-condoned. This includes the option of publicly attributing malicious cyber activity as a way of holding states to account. s6(a) [redacted]

Cyber security industry, research and skills

56. I would like the refresh of the Cyber Security Strategy and Action Plan to focus on steps to take advantage of the opportunities that cyber security represents. This includes expanding New Zealand's cyber security industry, investing in cyber security research and development, and dealing with the shortage of skilled cyber security workers. This will not only contribute to improving New Zealand's ability to protect our information systems, but support economic growth, including potentially in the regions and through exports. In this sense it is complementary to the suite of other initiatives I am advancing on digital technology.

57. There is potential for New Zealand to be recognised globally for its ability to manage the cyber security risk – and this could become a competitive advantage for the economy. A strong domestic cyber security sector would lift the cyber security of New Zealand's businesses and enhance New Zealand's reputation as a stable, innovative and safe environment in which to invest, find business partners, and do research and development. On the other side of the coin, countries that do not manage cyber security risks well may become increasingly unattractive as investment destinations due to perceptions of insecurity.

The security challenges of the Internet of Things and emerging technology

58. The refresh of the Cyber Security Strategy and Action Plan should also advise on the role that government should play in addressing the security challenges arising from the Internet of Things and other emerging technologies such as Artificial Intelligence or Quantum computing. This should include an assessment of the extent to which such technologies are empowering criminals and malicious actors.

59. In this area, we will need to keep in step with our international partners, as well as build awareness and capability amongst individuals, businesses and organisations to mitigate risks.

Next steps

60. If you agree, I intend to commission the National Cyber Policy Office within the Department of the Prime Minister and Cabinet to lead a comprehensive refresh of the Cyber Security Strategy and Action Plan. Proposed Terms of Reference for this work are attached as Annex One.

61. I would then report back to this Committee by 31 July with proposals for a refreshed Cyber Security Strategy and Action Plan that will provide a framework for intensified government initiatives to improve New Zealand's cyber security and realise the benefits of connectivity and digital innovation.

Consultation

62. The following departments were consulted: the Government Communications Security Bureau (including National Cyber Security Centre); New Zealand Security Intelligence Service; Department of Internal Affairs (including the Government Chief Digital Officer); Ministry of Business, Innovation and Employment (including CERT NZ); Ministry of Justice; Ministry of Defence; New Zealand Defence Force; Ministry of Foreign Affairs and Trade; NZ Police; and State Services Commission. The Treasury has been informed.

Financial Implications

63. This paper does not have any direct financial implications. The refresh can be conducted within existing resources. It is likely that some elements of a revised Cyber Security Strategy and Action Plan will require funding. Officials will engage with Treasury on these elements.

Human Rights

64. The current Strategy explicitly acknowledges as a core principle the protection of human rights when addressing cyber security issues. I intend to maintain this approach and ensure that cyber security is consistent with the Government's promotion and protection of digital rights.

Legislative Implications

65. Officials expect there may be legislative implications arising from the work to test the legislative framework in relation to cybercrime (paragraph 51) and to consider accession to the Budapest Convention (paragraph 53). Depending on other initiatives proposed in the refreshed Cyber Security Strategy and Action Plan, there may be additional legislative implications.

Regulatory Impact Analysis

66. There are no regulatory implications.

Gender Implications

67. There are no gender implications.

Disability Perspective

68. There are no disability implications.

Publicity

69. If approved, I will make an announcement about the decision to refresh the Cyber Security Strategy and Action Plan.

Recommendations

70. The Minister of Broadcasting, Communications and Digital Media recommends that the Committee:

1 **note** that in November 2015, Cabinet approved a new Cyber Security Strategy and Action Plan [NSC-15-Min-0012];

2 **note** that the Cyber Security Strategy, Action Plan and associated National Plan to Address Cybercrime, have provided an overarching framework for cross-government work under four goals (cyber resilience, cyber capability, addressing cybercrime, and international cooperation) and there has been good progress;

3 **note** that New Zealand is affected by increasing malicious cyber activity, with widespread use of connected devices and emerging technology intensifying the challenge;

4 **note** that, in the face of increasing malicious cyber activity, cyber security is essential to building a connected nation, promoting digital rights, online trust and confidence, and harnessing the value of digital technology for economic growth, community benefit and innovation;

5 **note** that I intend to develop a Digital Strategy for New Zealand in order to achieve a joined up response by government to digital technologies;

6 **agree** that, complementary to the planned Digital Strategy and the government's other digital initiatives, it is timely to undertake a comprehensive refresh of New Zealand's cyber security settings to ensure that we are investing the right resources in the right way across government to respond to growing cyber security threats;

7 **direct** the National Cyber Policy Office within the Department of the Prime Minister and Cabinet to lead this refresh in close collaboration with the full range of relevant government agencies, private sector and non-government organisation partners, and analysis of international best practice;

8 **agree** that the refresh of New Zealand's Cyber Security Strategy and Action Plan will propose new actions to improve New Zealand's cyber security, including possible recommendations in the following areas:

8.1 institutional cyber security arrangements;

8.2 government information security;

8.3 addressing cybercrime;

8.4 cyber diplomacy, deterrence s6(a)

8.5 opportunities in cyber industry, research and skills;

8.6 the security challenges of emerging technology;

9 **endorse** the attached Terms of Reference for the refresh of New Zealand's Cyber Security Strategy and Action Plan; and

10 **invite** the Minister of Broadcasting, Communications and Digital Media to report back to this Committee in July 2018 with a revised Cyber Security Strategy and Action Plan;

Hon Clare Curran
Minister of Broadcasting, Communications and Digital Media

Date:

Annex One: Terms of Reference for the Refresh of New Zealand's Cyber Security Strategy and Action Plan

Objectives of the 2015 Cyber Security Strategy and Action Plan

The 2015 Cyber Security Strategy and Action Plan provides a framework for cross-government and private sector work on cyber security. The Strategy sets a vision of "a secure, resilient and prosperous online New Zealand."

The Strategy is underpinned by four principles (partnerships are essential; economic growth is enabled; national security is upheld; and human rights are protected online).

The accompanying Action Plan sets out a number of actions under four goals (cyber resilience, cyber capability, addressing cybercrime and international cooperation) involving a wide range of agencies.

Objectives

The purpose of the refresh is to take a comprehensive look at New Zealand's cyber security framework and settings.

This work will result in a refreshed Cyber Security Strategy and Action Plan, which will provide a framework for intensified government initiatives to improve New Zealand's cyber security.

Problem definition

The current Cyber Security Strategy and Action Plan were developed in 2015. Since then, although there has been significant progress in the implementation of the Strategy and Action Plan, there has also been an upwards trajectory in cyber threats. The widespread use of Internet connected devices and emerging technology has intensified the challenge. Our Five Eyes partners, and other like-minded states, have strengthened their cyber security efforts.

It is timely to take a fresh look at the Cyber Security Strategy and accompanying Action Plan to test whether New Zealand is investing the right resources across intelligence, protective security, military, law enforcement and civilian agencies to respond effectively to growing cyber security threats.

Context

The National Cyber Policy Office within the Department of the Prime Minister and Cabinet leads the development of cyber security advice for the government and advises the government on the investment of resources in cyber security activities. The NCPO will lead the refresh of the Cyber Security Strategy and Action Plan.

Cyber security issues intersect with the work of a wide range of other government agencies including in the areas of national security and intelligence, defence, international relations, trade, economic development and innovation, criminal justice, education, government digital transformation, and public service delivery. The refresh will involve collaboration across a wide range of agencies to ensure a systemic approach to cyber security. It will also involve close collaboration with the private sector and non-government organisations.

The government has committed to building a connected nation, promoting and protecting digital rights, and harnessing digital technology for economic growth, community benefit and innovation. Cyber security will be critical to this. The refresh of the Cyber Security Strategy and Action Plan will intersect closely with the government's initiatives in the digital technology area.

Scope

The refresh of the Cyber Security Strategy and Action Plan will assess the nature of the cyber security risk, including the implications of emerging technology, and examine international best practice in cyber security strategies and action plans.

In view of the assessment of the cyber security threat and examination of international best practice, the refresh will test whether the vision, principles, and goals of the 2015 Cyber Security Strategy remain appropriate and make recommendations for any amendments.

It will include analysis of any gaps and obstacles in New Zealand's approach to cyber security as set out in the current Action Plan. This includes considering whether we are investing the right resources in the right places and have the right operational arrangements to deliver optimal coordinated effort across government.

It will include proposing new actions to address these gaps and obstacles. It may include recommendations about resources and institutional arrangements. The refresh will also outline current actions that must continue to contribute to New Zealand's cyber security. A refreshed Action Plan should comprise these new actions and on-going current actions.

It is envisaged that new actions proposed in a revised Action Plan will be the subject of subsequent more detailed policy and implementation processes as required.

Process

The National Cyber Policy Office within the Department of the Prime Minister and Cabinet will lead the refresh.

The NCPO will establish and chair a "Cyber Security Strategy and Action Plan Refresh Working Group" (the Working Group) including representatives from the following agencies amongst others: GCSB, CERT NZ, MFAT, NZ Police, GCDO and SSC.

This Working Group will engage with a broader range of other agencies as appropriate including but not limited to NZSIS, MBIE, DIA, GCDO, NZDF, MOD, MoJ, NAB, Customs, Statistics NZ (and the Government Chief Data Steward), MoE, TEC, NZQA, and NZTE. The Working Group will also engage with the Chief Technology Officer.

If any machinery of government issues arise, the Working Group will work closely with SSC and other agencies as appropriate. The Working Group will also ensure TSY is engaged on any initiatives that might require funding.

Consultation

The Cyber Security Strategy and Action Plan Refresh Working Group will work closely with government agencies, the Chief Technology Officer, the Human Rights Commissioner, the Privacy Commissioner, the Inspector-General of Intelligence and Security, non-government organisations and the private sector. Engagement with the private sector and other stakeholders can occur through the Connect Smart partnership – a community of practice to drive improved cyber security in New Zealand – and more widely as needed.

Relevant Ministers will be consulted on the revised Cyber Security Strategy.

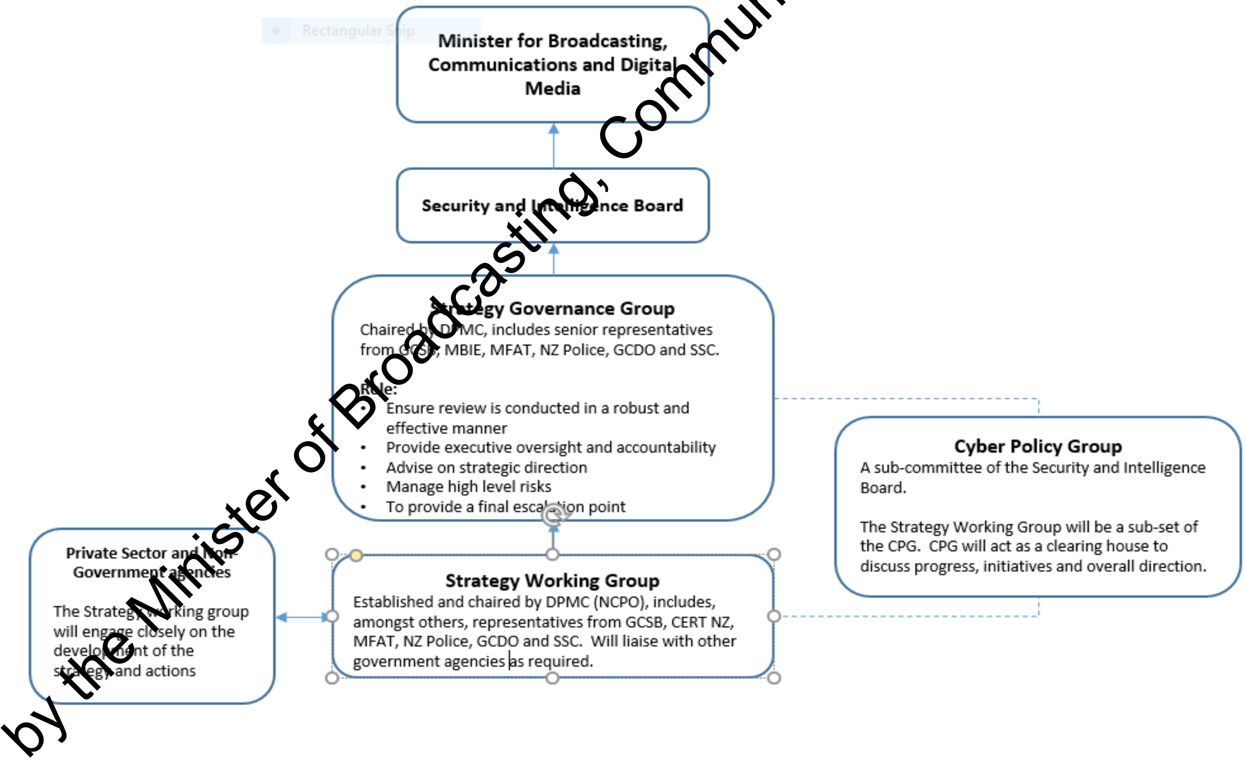
Governance

A “Cyber Security Strategy and Action Plan Refresh Governance Group” (the Governance Group) will be established to ensure the refresh is conducted in a robust and effective manner, provide executive oversight and accountability; and advise on strategic direction. The Governance Group will include senior representatives from DPMC, GCSB, MBIE, MFAT, NZ Police, GCDO, SSC and other agencies as necessary.

The Prime Minister, as Minister for National Security and Intelligence, has allocated cyber security policy responsibilities in her portfolio to the Minister of Broadcasting, Communications and Digital Media. This responsibility includes oversight and ongoing development of New Zealand’s Cyber Security Strategy, and the work programme related to this.

The recommendations for the refreshed Cyber Security Strategy and Action Plan will be submitted to the Minister of Broadcasting, Communications and Digital Media at the beginning of July 2018, to enable report back to the Cabinet External Relations and Security Committee by 31 July 2018.

Changes can be made to the terms of reference through agreement with the Minister of Broadcasting, Communications and Digital Media.



Minister for Broadcasting, Communications and Digital Media

Security and Intelligence Board

Strategy Governance Group
Chaired by DPMC, includes senior representatives from GCSB, MBIE, MFAT, NZ Police, GCDO and SSC.

Role:
- Ensure review is conducted in a robust and effective manner
- Provide executive oversight and accountability
- Advise on strategic direction
- Manage high level risks
- To provide a final escalation point

Cyber Policy Group
A sub-committee of the Security and Intelligence Board.

The Strategy Working Group will be a sub-set of the CPG. CPG will act as a clearing house to discuss progress, initiatives and overall direction.

Private Sector and Non-Government agencies

The Strategy working group will engage closely on the development of the strategy and actions

Strategy Working Group
Established and chaired by DPMC (NCPO), includes, amongst others, representatives from GCSB, CERT NZ, MFAT, NZ Police, GCDO and SSC. Will liaise with other government agencies as required.

Deliverables

- The National Cyber Policy Office will provide a report to the Minister of Broadcasting, Communications and Digital Media with recommendations for a revised Cyber Security Strategy and Action Plan at the beginning of July 2018.

- The Minister of Broadcasting, Communications and Digital Media will report back to the Cabinet External Relations and Security Committee by 31 July 2018 with a revised Cyber Security Strategy and Action Plan.

Annex Two: The cyber security role of government agencies

Cyber security issues intersect with the work of a wide range of other government agencies including in the areas of national security and intelligence, defence, international relations, trade and economic development, criminal justice, education, government digitalisation, and public service delivery. The key agencies include:

- The **National Cyber Policy Office** (NCPO) was established within the Department of the Prime Minister and Cabinet in 2012. It leads the development of cyber security policy advice for the government and advises the government on its investment of resources in cyber-security activities. It also engages with the private sector on cyber policy issues and leads New Zealand's engagement on international cyber policy matters (with the Ministry of Foreign Affairs and Trade). The NCPO developed the 2015 *Cyber Security Strategy and Action Plan* and oversees its implementation.

- The **Government Communications Security Bureau**, through the **National Cyber Security Centre** (NCSC), detects, disrupts and responds to cyber threats against public and private sector organisations of national significance. It delivers cyber threat intelligence to customers and partners. GCSB information assurance activities include providing high-grade encryption services to protect classified information and assessing proposed outer space and high altitude activity and changes to telecommunications networks for risks to national security. It also provides information assurance and security guidance to government agencies including through the Information Security Manual, which is an integral component of the Protective Security Requirements.

- The **New Zealand Security Intelligence Service** (NZSIS) delivers the Protective Security Requirements, which includes information security, for government agencies.

- **New Zealand Police** addresses cybercrime (particularly through the Police Cybercrime Unit within the High Tech Group), which is one of the four goals of the *Cyber Security Strategy*.

- The **Ministry of Justice** (MOJ) works on the rule of law and justice sector policy, including oversight of the *Harmful Digital Communications Act 2015* and the review of the *Privacy Act 1993* – the latter includes proposals on data breach reporting.

- The **Ministry of Business, Innovation and Employment** (MBIE) links with cyber security in the areas of communications policy, the Digital Economy Work Programme, research and innovation, consumer advice, and support for small businesses. MBIE advises the Minister for Communications on the implementation of 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.

- **CERT NZ** receives reports of cyber incidents, analyses threats, shares information and advice, coordinates incident responses, and is a point of contact for the international CERT community. CERT NZ has been set up, initially, as a branded business unit within MBIE.

- The **Department of Internal Affairs** (DIA) is the home of the Government Chief Digital Officer – the functional lead for the government's information communications technology strategy. The Department of Internal Affairs includes the Electronic Messaging Compliance Unit (anti-spam) and Censorship Compliance Unit.

- The **Ministry of Foreign Affairs and Trade** (MFAT) works jointly with NCPO on cyber security diplomacy, including cyber security dialogues with other countries, advancing norms of state behaviour online, promoting the applicability of international law in cyber space, and addressing barriers to trade arising from other countries' cyber security regulations. International cooperation is one of the four goals of *New Zealand's Cyber Security Strategy*.

- The **Ministry of Defence** (MOD) and the **New Zealand Defence Force** (NZDF) are focused on building the cyber capabilities required to support New Zealand's military operations, including the protection of the NZDF domestic and deployed networks s6(a)