SUMMARY OF NEW ZEALAND'S Cyber Security Strategy:

A secure, resilient and prosperous online New Zealand

New Zealand is increasingly reliant on information communication technology and an open, trusted Internet. Internet connectivity is an integral part of New Zealand's economic growth and international competitiveness.

But this technology provides opportunities for those with criminal or hostile intentions. The 2015 Cyber Security Strategy signals the government's commitment to ensuring New Zealand is safe, resilient and prosperous online.

New Zealand's scale and relatively simple telecommunications and network structure enables the public and private sector to work closely together to embed a cyber security culture, and to respond nimbly to evolving cyber risks.

WHAT IS CYBERSPACE?

The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.

Cyber Security Goals

FOUR INTERSECTING GOALS WILL CREATE A SECURE, RESILIENT AND PROSPEROUS ONLINE NEW ZEALAND:

CYBER RESILIENCE

New Zealand's information infrastructures can resist cyber threats and we have the tools to protect our national interests

CYBER CAPABILITY

New Zealanders, businesses and government agencies understand cyber threats and have the capability to protect themselves

NEW ZEALAND'S Cyber Security Strategy

ADDRESSING CYBERCRIME

New Zealand improves its ability to prevent, investigate and respond to cybercrime

INTERNATIONAL COOPERATION

New Zealand protects and advances its interests on cyberspace issues internationally

Principles underpinning the Cyber Security Strategy

PARTNERSHIPS ARE ESSENTIAL

The government has a role to play in cyber security – but not on its own. Close partnerships with the private sector and non-government organisations are required. Businesses drive the New Zealand economy and depend on the Internet and networked technology. They must protect the information that is critical to their commercial success. The private sector owns and operates the telecommunications systems. The private sector and technical community also have considerable cyber security expertise.

The Connect Smart partnership is a public-private collaboration focused on driving cyber security improvement in New Zealand. Connect Smart includes a growing network of banks, telecommunication companies, ICT companies, software companies, social media, retail organisations, education institutions, non-government organisations, community groups, sectoral bodies, business associations and government agencies.

ECONOMIC GROWTH IS ENABLED

Strong cyber security practices will result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, innovate and invest.

ICT and enhanced connectivity will continue to boost economic growth, and the costs of cyber insecurity will be minimised.

NATIONAL SECURITY IS UPHELD

Cyber threats to New Zealand – particularly state-sponsored espionage, cyber terrorism, theft of intellectual property from government and critical national infrastructure – are national security risks. Upholding New Zealand's national security in the face of this threat is a fundamental principle of this Strategy.

HUMAN RIGHTS ARE PROTECTED ONLINE

The openness of the Internet is part of its unique value – allowing for unrestricted participation and the free flow of information.

Cyberspace should be a trusted medium, where users have confidence in the integrity of information and the protection of their private and financial details. They should be able to engage online without suffering harm or unlawful interference.

Human rights apply online as they do offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law.

Cyber Security Strategy Action Plan

The Cyber Security Strategy is accompanied by a living Action Plan. This Plan will evolve to keep pace with technology developments and the emergence of new threats. New actions may be added, and existing actions amended. The National Cyber Policy Office will work with government agencies and Connect Smart public-private cyber security partners to produce a public annual report on progress.

CYBER RESILIENCE

- Set up a national CERT[1]
- Vigorously protect New Zealand's most important information infrastructures
- Use cyber tools to further New Zealand's national security interests
- Prepare for major cyber incidents

CYBER CAPABILITY

- Expand Connect Smart activities and partnership
- Improve the cyber security capability of small and medium enterprises
- Boost the cyber security capability of the corporate sector, including national infrastructure, and the public sector
- Promote cyber security education and training, including building a cyber security professional workforce
- Support cyber security research and business innovation

ADDRESSING CYBERCRIME

- Build capability to address cybercrime
- Adapt New Zealand's policy and legislative settings for the digital age
- Enhance New Zealand's operational response to cybercrime
- Use New Zealand's international connections to fight cybercrime

INTERNATIONAL COOPERATION

- Promote internet governance and norms of state behaviour that reflect New Zealand's interests
- Build networks of international operational cooperation
- Contribute to international cyber security capability and confidence
- Maximise the economic opportunities of cyberspace for New Zealand and New Zealanders

[1] CERT was once an acronym for 'computer emergency response team'. Since 1997, CERT has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym. New Zealand is requesting permission to use the CERT trademark.