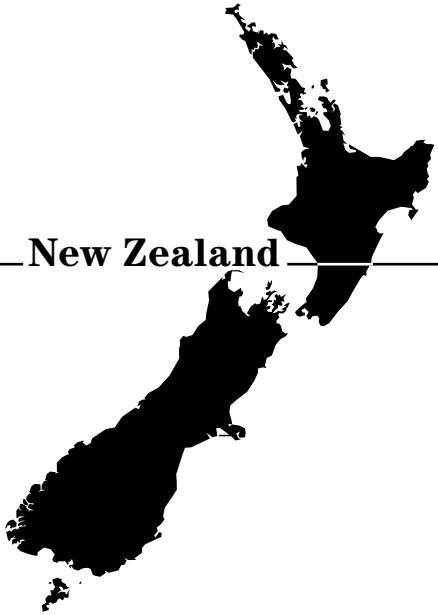
CIIP Country Surveys



New Zealand

The Country Survey of New Zealand 2004 was written with the help of Mike Harmon, Centre for Critical Infrastructure Protection (CCIP).

New Zealand

Critical Sectors

CIIP in New Zealand is about the protection of infrastructure necessary to provide critical services. "Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement."[288] New Zealand's critical sectors comprise the assets and systems required for the maintenance of:[289]

- Emergency Services,
- Energy (including Electricity Generation and Distribution, and the Distribution of Oil and Gas),
- Finance and Banking,
- Governance (including Law and Order and National and Economic Security),
- Telecommunications and the Internet,
- Transport (including Air, Land, and Sea).

Various critical sectors depend on each other. Most systems assume the continuity of power and telecommunications infrastructures and make extensive use of networked information technology in their management and control systems.

Initiatives and Policy

The New Zealand government's *Defence Policy Framework* is a crucial document that illustrates that CIIP is a key objective of the country's overall security policy. The *Centre for Critical Infrastructure Protection* (CCIP) addresses the cyber-threat aspects of that objective.

288 http://www.ccip.govt.nz/about-ccip/niip-report-final.htm#_Toc501363182.

289 E-Government Unit, State Services Commission. *Protecting New Zealand's Infrastructure from Cyber-Threats* (8 December 2000). http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.

CIIP within the Defence Policy Framework

New Zealand's government promotes a comprehensive approach to security and aims to protect and maintain the country's physical, economic, social, and cultural security. In the government's *Defence Policy Framework* of June 2000, critical infrastructure protection is identified as one of the key objectives: "[…] to defend New Zealand and to protect its people, land, territorial waters, Exclusive Economic Zone, natural resources and critical infrastructure."[290]

Protecting New Zealand's Infrastructure from Cyber-Threats

On 8 December 2000 the report *Protecting New Zealand's Infrastructure from Cyber-Threats* was released by New Zealand's *State Services Commission's E-Government Unit*. The report deals with the protection of New Zealand's critical infrastructure from cyber-crime and other IT-based threats. The report assessed levels of risk due to IT-based threats in finance and banking, transport, electric power, telecommunications and the Internet, oil and gas, water, and critical State services that support national safety, security, and income.[291] The report made several recommendations such as:

- the establishment of a New-Zealand-based security-monitoring and incident-handling organization,
- the harmonization of computer-crime legislation with that of other nations (e.g., Australia, the United States, United Kingdom and Canada),
- the adoption of specific IT security standards,
- the establishment of an ongoing cooperation program between owners of critical infrastructure and the government.[292]

290 Minister of Defence. *The Government's Defence Policy Framework* (June 2000), p. 4: http://www.executive.govt.nz/minister/burton/defence/index.html. Or: http://www.defence.govt.nz/public_docs/defencepolicyframework-June2000.pdf.

291 Minister of State Services, 11 February 2001. Media Release on Cyber Crime. http://www.ccip.govt.nz/about-ccip/media-release-cyber-crime.htm.

292 E-Government Unit, State Services Commission, 8 December 2000. *Protecting New Zealand's Infrastructure from Cyber-Threats*. http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.

Centre for Critical Infrastructure Protection (CCIP)

On 11 June 2001, the report *Towards a Centre for Critical Infrastructure Protection* (CCIP) was issued by the *E-Government Unit.*[293] It recommended the establishment of a Centre for Critical Infrastructure Protection by the government. The argument was that the dependence of citizens and businesses on various infrastructure services, the vulnerability of IT systems, and the increasing risks and possible damages caused in case of failure were increasing. Therefore, measures must be taken to ensure that infrastructure operators and government agencies are kept up to date on vulnerability and threat information: "The CCIP is proposed as an insurance measure in that it mitigates, for a low cost, a risk of a large loss."[294]

In the early stages of CCIP planning, the location of the new centre was constrained by a) the need to give private-sector companies the confidence that their sensitive commercial and security information would be adequately safeguarded, and by b) the need to provide a secure environment to adequately protect intelligence information to which the CCIP must have access. It was stated that "Overseas experience shows that the Centre should not be part of a law-enforcement agency, since this might reasonably focus on the pursuit of offenders to the detriment of rectifying damage and of confidentiality."[295] The *Government Communications Security Bureau* (see below) was finally appointed on the basis of cost, effectiveness and because of its significant IT security skills and its culture of security.[296]

Furthermore, the E-Government Unit acknowledged that timely access to classified intelligence, among other sources, would be necessary for the CCIP to provide the best chance of a successful threat warning.[297]

293 E-Government Unit, State Services Commission. *Towards a Centre for Critical Infrastructure Protection* (11 June 2001). http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

294 Ibid., p. 5.

295 Cabinet Paper. *Centre for Critical Infrastructure Protection* (13 August 2001), pp. 5, 9–11: http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.

296 Ibid., and: Towards a Centre for Critical Infrastructure Protection, 11 June 2001, p. 2. http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

297 Towards a Centre for Critical Infrastructure Protection, 11 June 2001, p. 9. http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

Security in the Government Sector

The *Interdepartmental Committee on Security* in 2002 issued a comprehensive and detailed manual called '*Security in the Government Sector*', which took into account the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 "Information Technology – Code of Practice for Information Security Management" dealing with possible sources of threats to information and how to counter them. The manual's security guidelines were made mandatory for government departments, ministerial offices, the *New Zealand Police*, the *New Zealand Defence Force*, the *New Zealand Security Intelligence Service*, and the *Government Communications Security Bureau*. In the manual, the government requires information important to its functions, its official resources, and its classified equipment to be adequately safeguarded to protect the public and national interests and to preserve personal privacy.[298]

Furthermore, the manual proposes that overall responsibility for security rest with a manager, designated as *Departmental Security Officer* (DSO). That person's duties should include the formulation and implementation of the general security policy and common minimum standards within the organization, to issue instructions on security, and to serve as liaison with the *Secretary of the Interdepartmental Committee on Security* (ICS), the *New Zealand Security Intelligence Service* (NZSIS), and the *Government Communications Security Bureau* (GCSB) for any special advice.[299]

Security Policy and Guidance Website

The security policy and guidance website (*www.security.govt.nz*) provides information on the governments action concerning information security. This website acts as a focal point for the publication of government information about security standards, procedures and resources.[300]

298 Department of the Prime Minister and Cabinet. *Security in the Government Sector* (2002). http://www.security.govt.nz/sigs/index.html.

299 Ibid., Chapter 2.

300 http://www.gcsb.govt.nz/infos/infos02.htm.

Standards New Zealand (SNZ)

Standards New Zealand (SNZ) [301] promotes several New Zealand specific standards as well as a host of joint Australian/New Zealand and international standards. AS/NZS ISO/IEC 17799 Information Security Management provides an overview of factors to be considered and included in the protection of information and information systems.

Organizational Overview

Public Agencies

The Domestic and External Security Secretariat (DESS)

The main actor in charge of formulating New Zealand's security policy, including CIIP, is the *Domestic and External Secretariat* (DESS), which co-ordinates central government activities aimed at protecting New Zealand's internal and external security, including intelligence, counter-terrorism preparedness, emergency and crisis management, and defense operations. The DESS director provides timely advice to the prime minister on issues affecting the security of New Zealand, including policy, legislative, operational, and budgetary aspects. DESS is the support secretariat for the *Officials Committee for Domestic and External Security Co-ordination*.[302]

Officials Committee for Domestic and External Security Co-ordination (ODESC)

The *Officials Committee for Domestic and External Security Co-ordination* (ODESC) is chaired by the prime minister and makes high-level policy decisions on security and intelligence matters, including policy oversight in the areas of intelligence and security, terrorism, maritime security, and emergency preparedness. ODESC comprises chief executives from the *Ministry of Foreign Affairs and Trade*, the *Ministry of Defence* and the *Defence Force*, the *New Zealand Security Intelligence Service*, the *Government Communications Security Bureau*, the *Police*, the *Ministry of Civil Defence and Emergency Management*, *Treasury*, and others when necessary.[303]

301 http://www.standards.co.nz.
302 http://www.dpmc.govt.nz/dess/index.htm.
303 http://www.dpmc.govt.nz/dess/index.htm.

Interdepartmental Committee on Security (ICS)

The *Interdepartmental Committee on Security* (ICS)[304] is a sub-committee of the *Officials Committee for Domestic and External Security Co-ordination* (ODESC). It formulates and coordinates the application of all aspects of security policy and sets common minimum standards of security and protection, which all government organizations must follow. In addition, the ICS provides detailed advice on information security matters to government and other organizations or bodies that receive or hold classified information.[305]

Centre for Critical Infrastructure Protection (CCIP)

The *Centre for Critical Infrastructure Protection* (CCIP) was established in 2001 to provide advice and support to public and private owners of CI, in order to protect New Zealand's critical infrastructure from cyber-threats. The CCIP is located within the *Government Communications Security Bureau* and has three main tasks:

- To provide a round-the-clock vigilance and advice service to owners of critical infrastructure and to government departments,
- To analyze and investigate cyber-attacks, and
- To collaborate with national and international critical infrastructure organizations to improve awareness and communications regarding information technology security.[306]

Whereas the CCIP provides coordination, support, and advice on the ways in which information security can be maintained and improved, owners of critical infrastructures in the public and private sectors will remain responsible for the security of their own systems.[307]

Government Communications Security Bureau (GCSB)

The CCIP is part of the *Government Communications Security Bureau* (GCSB). In 1977, the *Combined Signals Organization* was replaced by the current signals intelligence agency – the GCSB, which is a civilian organization. Its chief executive reports directly to the prime minister. The GCSB

304 http://www.security.govt.nz.

305 Department of the Prime Minister and Cabinet. *Security in the Government Sector* (2002). http://www.security.govt.nz/sigs/chapter-1-security-policy.doc. http://www.security.govt.nz/sigd/sigd2a.html.

306 http://www.ccip.govt.nz/about-ccip/about-ccip.htm.

307 Cabinet Paper. Centre for Critical Infrastructure Protection, 13 August 2001: http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.

gives advice and assistance to New Zealand government departments and agencies concerning the security of information-processing systems.[308]

One of the GCSB's tasks is to ensure the integrity, availability and confidentiality of official information through the provision of *Information Systems Security* (INFOSEC) services to departments and agencies of the New Zealand government, and to contribute to the protection of the critical infrastructure from IT threats.[309] The *New Zealand Security of Information Technology* (NZSIT) publications are therefore produced as guidelines for New Zealand government organizations in support of securing and protecting IT systems and associated information and services.[310]

E-Government Unit

The E-Government Unit was established in July 2000 in the *State Services Commission* (a department of the New Zealand Public Service[311]). The following projects are under the umbrella of this unit:

- A *Secure Electronic Environment* (S.E.E.) for the protection of sensitive information within and among government agencies. A sub-project of the S.E.E. project is the development of a framework for authentication in accessing sensitive systems within public key infrastructures. The intention is to develop minimum requirements and a framework for the accreditation of certification authorities;
- The study "*Protecting New Zealand's Infrastructure From Cyber-Threats*" on national critical infrastructures and their level of vulnerability to cyber-threats.

Public Private Partnerships

New Zealand Security Association (NZSA)

The *New Zealand Security Association* (NZSA) was formed in 1972 and represents licensed and certificated persons providing services to government departments, state-owned enterprises, businesses, and private users. The NZSA has two member groups: Corporate members, who are individu-

308 Domestic and External Security Secretariat. *Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies* (December 2000). http://www.dpmc.govt.nz/dess/securingoursafety/index.html.

309 http://www.gcsb.govt.nz/function.htm.

310 http://www.gcsb.govt.nz/nzsit/index.htm.

311 http://www.ssc.govt.nz/display/home.asp.

als or companies engaged in the security industry, and associate members, who are individuals or companies involved or interested in security without offering the services to the public. Members of the latter category include government departments, insurance companies, airlines, banks, food distributors, area health boards, oil companies, etc.[312] Among the NZSA's main objectives are:

- To set minimum operating standards for members and developing and approving codes of practice,
- To co-operate with the police, government departments, and agencies and other organizations concerned with the safekeeping of people, property, and information in New Zealand,
- To provide information and advisory services, education, and training.[313]

Computer Society Special Interest Group on Security (NZCS SigSec)

The *New Zealand Computer Society's Special Interest Group on Security* (NZCS SigSec) is a forum for networking with others with an interest in IT security from within and outside government. It meets quarterly for a presentation and networking.[314]

Early Warning Approaches

AusCERT

AusCERT[315] is the national *Computer Emergency Response Team for Australia* and also provides significant support to New Zealand organizations. It is one of the leading CERTs in the Asia/Pacific region; it provides prevention, response, and mitigation strategies for members.[316]

AusCERT was founded as a commercial CERT for Australia before the New Zealand *Centre for Critical Infrastructure Protection* (CCIP) was formed. The CCIP has a working relationship with AusCERT, but also

312 http://www.yellow.co.nz/site/newzealandsecurityassociation/.
313 http://www.security.org.nz/nzsa/aboutus.htm.
314 http://www.nzcs.org.nz.
315 See also the Country Survey on Australia in this book.
316 http://www.auscert.org.au.

provides an early-warning service and a moderated mailing list through its website.

Several commercial organizations – including the New Zealand company Co-logic – also provide vulnerability alerts filtered and tailored for their customers.[317]

317 http://www.cologic.co.nz .

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger