



Government Communications Security Bureau

ANNUAL REPORT

for the year ended 30 June 2006

Presented to the House of Representatives pursuant to
Section 12 of the
Government Communications Security Bureau Act 2003

ISSN 1176-4686

LETTER OF TRANSMITTAL

Prime Minister

I have the honour to present to you the report of the Government Communications Security Bureau for the year ended 30 June 2006.

The report has been prepared for public release in accordance with the requirements of section 12(4) of the Government Communications Security Bureau Act 2003.



Warren Tucker
Director

TABLE OF CONTENTS

LETTER OF TRANSMITTAL	1
TABLE OF CONTENTS	2
DIRECTOR'S OVERVIEW.....	3
STATEMENT OF PURPOSE	5
MISSION AND OUTCOMES.....	6
Vision	6
Mission Statement	6
Outcomes	7
THE YEAR IN REVIEW	8
ACHIEVEMENT OF OUTCOMES	9
Provision of Intelligence and Threat Warning Information	9
Protecting Official Information and the Critical National Infrastructure	10
Statement on Interception Warrants.....	12
Statement on Computer Access Authorisations.....	12
Oversight and Review	12
Internal Audit	12
Legal and Statutory	12
ORGANISATIONAL INFORMATION.....	13
Corporate Structure	13
People Capability.....	14
STATEMENT OF RESPONSIBILITY.....	17
STATEMENT OF EXPENDITURE AND APPROPRIATION	18
AUDIT REPORT	19

Part One

Director's Overview

DIRECTOR'S OVERVIEW

This year has again been very busy as the Bureau has worked both to deliver its services to Government, and to further enhance its capabilities against the backdrop of a demand for a widening range of foreign intelligence and information systems security services.

Counter-terrorism and regional issues continue to be the major focuses of the Bureau's intelligence efforts in support of the Government's foreign intelligence requirements.

Developments during the year included implementation of enhanced technical capacity at both collection stations, completion of the first phase of the New Zealand Intelligence Community Network, the further development of the GCSB's role in support of the New Zealand Defence Force, and the development of a new operations strategy that will ensure that the Bureau remains well placed to carry out its statutory functions as set out in the Government Communications Security Bureau Act 2003.

A continuing focus throughout the year has been the ongoing development of our relationships with key customers. The Bureau has also provided support to Ministers and senior officials at a number of international events, and to Police and other law enforcement agencies in relation to our statutory function of providing support to the prevention and detection of serious crime.

The Bureau's information systems security business increased in scope following last year's increase in staff and redesigned work processes. The external training programme was significantly enhanced, with a 100% increase in courses offered compared with the previous year. In addition, several significant publications were released, including the New Zealand Government IT Security Manual (NZSIT 400).

Internally, the Bureau made further progress with the implementation of its Human Resources Strategy, focussing this year on fine-tuning the Bureau's individual performance management system to align it more closely with our remuneration practice, and appointing a number of Learning Advisors to provide training in key aspects of the Bureau's operations.

In the Information and Communications Technology area, planning and implementation of enhancements in the reliability, capability and scalability of the Bureau's IT infrastructure continued.

This is my last Annual Report as Director GCSB. Looking back at the significant progress which Team GCSB has achieved during the seven years of my tenure as Director leaves me in no doubt that the Bureau is in very good shape as I prepare to depart. I have every confidence that the Bureau will continue to flourish in the years ahead.



Warren Tucker
Director

Part Two

Statement of Purpose

MISSION AND OUTCOMES

Vision

To provide world-class intelligence and information assurance services to the New Zealand Government.

Mission Statement

The mission of the GCSB is to contribute to the national security of New Zealand through:

- providing foreign signals intelligence¹ to support and inform Government decision making;
- providing an all-hours intelligence watch and warning service to Government;
- ensuring the integrity, availability and confidentiality of official information through information systems security services to Government; and
- contributing to the protection of the critical national infrastructure from information-borne threats.

¹ Foreign intelligence as defined in the GCSB Act 2003 means information about the capabilities, intentions or activities of a foreign organisation or a foreign power.

Outcomes

The Government purchases services from the Bureau to achieve its two high-level outcomes:

- New Zealanders and New Zealand interests are protected and advanced through the provision of relevant, timely and accurate foreign intelligence, and threat warning information; and
- National and public interest is properly served through the appropriate protection of official information and the critical national infrastructure.

The Bureau seeks to contribute to these outcomes through achieving four departmental outcomes as shown in the diagram below:

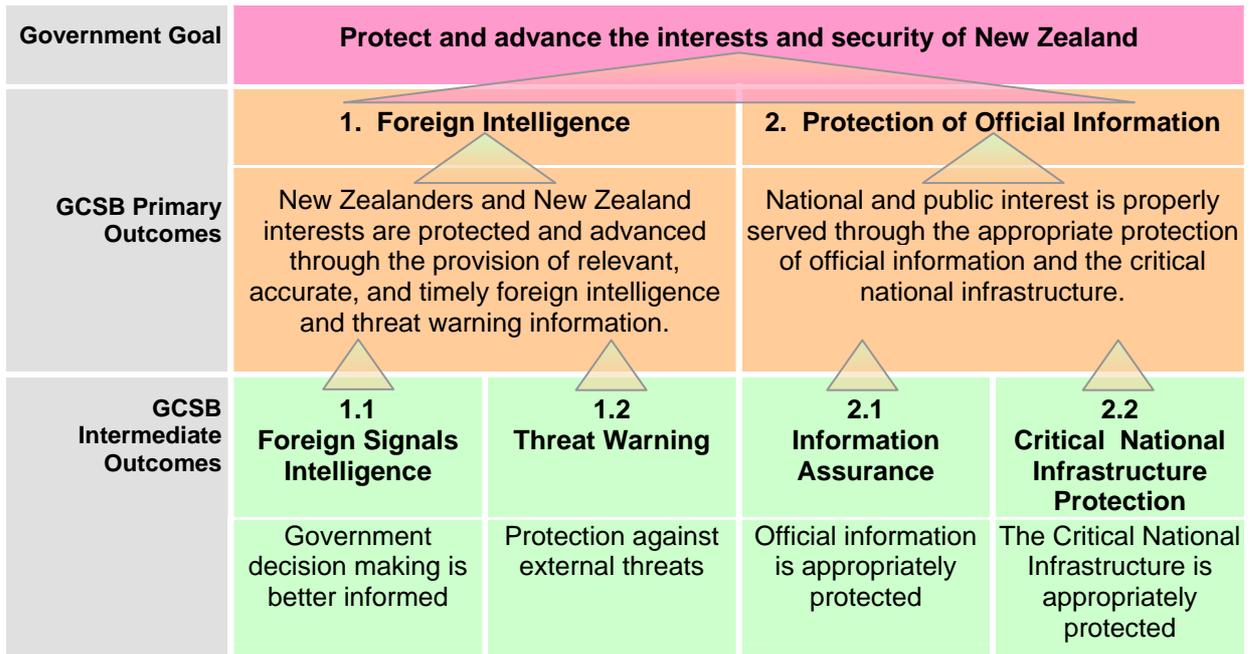


Figure 1 – GCSB Outcomes

Part Three

The Year in Review

ACHIEVEMENT OF OUTCOMES

Provision of Intelligence and Threat Warning Information

“New Zealanders and New Zealand interests are protected and advanced through the provision of relevant, accurate, and timely foreign intelligence, and threat warning information.”

Better Informing Government Decision-making

“Government decision making in relation to security and defence, international relations and economic well-being is better informed and advantaged through the provision of relevant, accurate, and timely foreign signals intelligence.”

The Bureau seeks to make a difference to Government decision-making in relation to security and defence, international relations and economic well-being through the provision of foreign intelligence. The demand for the Bureau’s services has continued to increase in response to the complexity of the international context in which New Zealand must operate.

The provision of foreign signals intelligence is driven by the New Zealand Government’s foreign intelligence requirements.

The GCSB operates two intercept stations at Tangimoana and Waihopai, both of which it is continuing to upgrade to preserve its ability to collect foreign intelligence from the rapidly-changing modern communications environment.

The Bureau’s volume of intelligence production is still trending upwards, though the number of reports dropped slightly during the year, in large part due to the cessation of a reporting stream that is no longer required.

A continued focus throughout the year was on increasing the level of intelligence support to other Government departments, in particular the New Zealand Defence Force.

Protecting New Zealanders and New Zealand Interests through Threat-warning

“New Zealanders and New Zealand interests are better protected from external threats and risks through the provision of timely alerts and threat warnings.”

The Bureau seeks to ensure that relevant agencies receive timely information that prevents or reduces a negative outcome such as the loss of life, or assists in the detection and prevention of serious crime with an international dimension. The Bureau achieves this through the operation of a 24 hour 7-day Operations Centre. This is frequently the means by which the New Zealand Government becomes aware of threats, particularly terrorist threats, and receives tip-off information on changing events.

The Bureau, in concert with integrated NZDF staff where appropriate, provides intelligence and threat warning support to NZDF military operations, and advice on intelligence matters to the NZDF and a range of other Government departments and agencies.

Protecting Official Information and the Critical National Infrastructure

“National and public interest is properly served through the appropriate protection of official information and critical national infrastructure.”

Appropriately Protecting Official Information

“Electronically stored, processed or transmitted information is appropriately protected through the application of information systems security.”

A key requirement for the Bureau is to ensure that official information is appropriately protected through the application of information systems security (INFOSEC) measures² from unauthorised access, disclosure or tampering. The Bureau seeks to achieve this by assisting departments to protect their official information through the provision of INFOSEC inspection services, training, policy and doctrine, cryptographic keying material, and the procurement of cryptographic equipment.

Demand for the Bureau’s INFOSEC education and training services remained high in all areas during the year, with training courses in particular building up to a 5-year peak of 41, as illustrated in Figure 2. As is the norm, departments and agencies handling and storing material at the CONFIDENTIAL level or higher, or in areas of increased INFOSEC threat, such as New Zealand’s posts and missions overseas, were a priority for assistance.

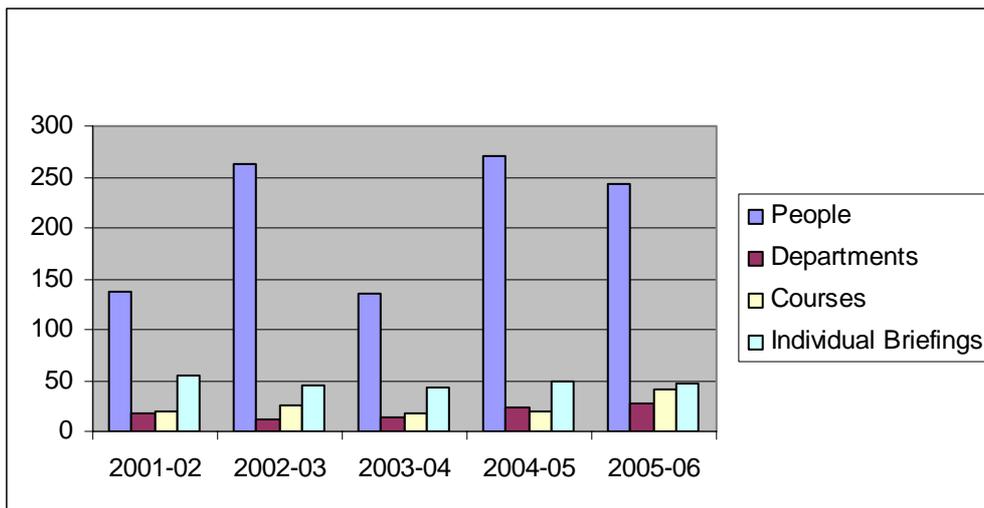


Figure 2 - INFOSEC Education and Training Services

During FY2005-06, the Bureau conducted 41 training courses involving 243 personnel representing 28 departments.

² The responsibility for protecting official information, however, remains that of the relevant Chief Executive.

Protecting Against Information-Borne Threats

“New Zealand’s security and well-being is enhanced through protection against information-borne threats.”

The Centre for Critical Infrastructure Protection (CCIP) has operated since 2002 to ensure that New Zealand’s critical information infrastructure does not fail due to “cyber-threats”. The Centre’s activities comprise a 24-hour 7-day watch-and-warn service, network analysis and advisory services, outreach and training programmes.

The CCIP cooperates with and advises a number of critical national infrastructure organisations and forums, closely liaises with international infrastructure protection agencies, and participates in international forums.

Nine significant cyber-incidents were reported to the CCIP during the year and acted on promptly. The Centre issued 649 alerts and advisories, from a wide variety of sources. Six CCIP newsletters were also published to customer organisations.

Significant initiatives during the year that will benefit New Zealand included:

- conducting New Zealand’s inaugural national Cyber Exercise as part of a wider, international exercise that included participants from both public and private sectors;
- participating as standing member of the Bankers’ Association Internet Fraud Forum; and
- establishing a connection with the International Watch and Warn Network – a 15 country operational collaboration portal for cyber-borne threats.

Statement on Interception Warrants

A number of Foreign Interception Warrants, issued pursuant to section 17 of the Government Communications Security Bureau Act 2003, were in force during the year ended 30 June 2006.

Statement on Computer Access Authorisations

A number of Computer Access Authorisations, issued pursuant to section 19 of the Government Communications Security Bureau Act 2003, were in force during the year ended 30 June 2006.

Oversight and Review

The GCSB (in common with the New Zealand Security Intelligence Service) is subject to oversight by the Inspector-General of Intelligence and Security, Hon Paul Neazor QC. The principal role of the Inspector-General is to assist the Minister in the oversight and review of New Zealand's intelligence and security agencies.

The GCSB consulted the Inspector-General on two issues during the year. The Inspector-General did not note any issues of concern relating to the GCSB during the reporting year.

The Intelligence and Security Committee is a statutory committee of Parliamentarians established by the Intelligence and Security Committee Act 1996. The Intelligence and Security Committee met three times during the year to consider, *inter alia*, the GCSB's Annual Report, budgetary estimates and Statement of Intent.

Internal Audit

The Bureau's Internal Audit function covers both the audit of selected performance issues and the maintenance of ongoing financial controls.

PriceWaterhouseCoopers is contracted by the Bureau to provide Internal Audit Finance functions. During the year PriceWaterhouseCoopers conducted three reviews as part of the internal audit programme. There were:

- Managing Costs and Outputs;
- Departmental Control Evaluation; and
- Budgeting and Planning.

PriceWaterhouseCoopers also carried out a follow up of the FY2004-05 review recommendations.

Legal and Statutory

The Bureau maintains a small legal and compliance team to provide advice on legal and statutory matters.

During the year the team provided advice on the application and interpretation of the GCSB Act.

ORGANISATIONAL INFORMATION

Corporate Structure

Description

The Bureau is divided into six functional areas:

- Intelligence Collection and Processing;
- Intelligence Production and Customer Services;
- Defence Relationship Management;
- Information Systems Security;
- Technology Support and Communications; and
- Corporate Services, Policy, Planning and Legal.

The Bureau has two collection or interception stations: the HF radio interception and direction-finding station at Tangimoana, and the satellite communications station at Waihopai, near Blenheim.

The Bureau's management structure is shown in the diagram below:

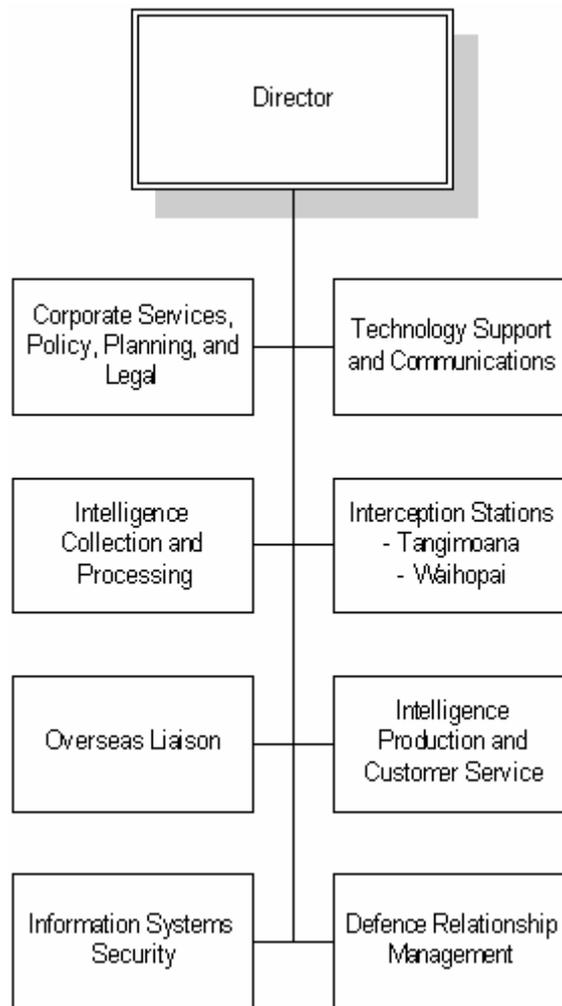


Figure 3 – GCSB Organisation

People Capability

Good Employer Requirements

The Bureau is a department of the Public Service, and operates in accordance with section 56 of the State Sector Act 1988, which requires departments to operate a personnel policy that complies with the principle of being a “good employer”. This requires departments to provide for the fair and proper treatment of employees in all aspects of their employment.

HR Strategy

The Bureau has made progress implementing the Human Resources Strategy by:

- fine-tuning the Bureau's individual performance management system to align it more closely with our remuneration practice; and
- appointing a number of Learning Advisers to provide training in key aspects of the Bureau's operations.

Encouraging Diversity within the GCSB

The Bureau recognises that understanding and knowledge of different perspectives enhances the performance of its employees and hence the organisation. In addition to complying fully with the Human Rights Act 1993, and the New Zealand Bill of Rights Act 1990, we are endeavouring to achieve this through:

- ensuring that all employees have equal access to employment opportunities;
- membership of the EEO Trust; and
- fostering of non-discriminatory practices within the GCSB's recruitment procedures.

Key achievements during the year included:

- continued networking and membership of the EEO Trust Employers' Group; and
- participation in an Employee Assistance Programme for all employees who choose to access the programme for advice and assistance.

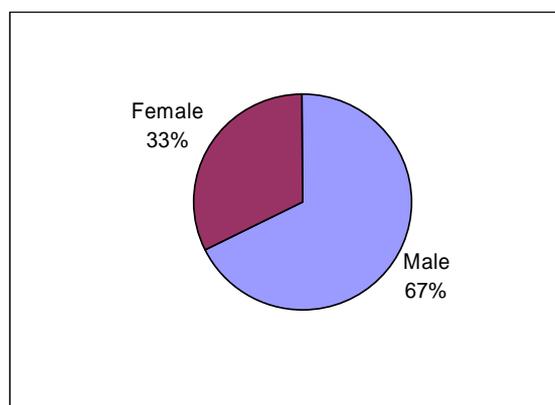


Figure 4 - Composition of Staff by Gender

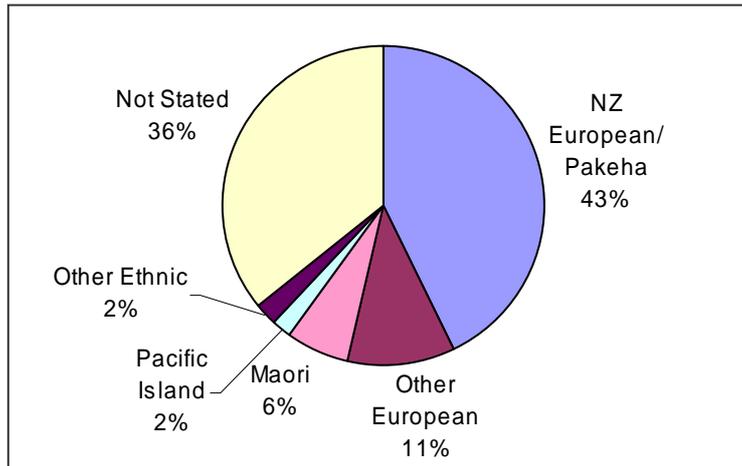


Figure 5 – Composition of Staff by Ethnicity

Operational Capacity – Staffing Numbers

The total number of staff employed in the GCSB at 30 June 2006 was 334, an increase of 5 staff over the total staff employed at 30 June 2005. Staff turnover (excluding fixed term and casual employees) increased from 3.9% to 9.3%.

Accommodation

A major project was commenced to plan for the Bureau's future Head Office accommodation requirements.

Part Four

Financial Reporting

STATEMENT OF RESPONSIBILITY

The Government Communications Security Bureau prepares annual financial statements in accordance with generally accepted accounting practice which fairly reflect the financial operations of the Bureau and the Bureau's financial position at the end of the financial year.

The financial statements are presented to the Intelligence and Security Committee.

In terms of sections 35 and 37 of the Public Finance Act 1989, I am responsible as Chief Executive of the Government Communications Security Bureau, for the preparation of the Bureau's financial statements and the judgements made in the process of producing those statements.

I have the responsibility of establishing and maintaining, and I have established and maintained, a system of internal control procedures that provide reasonable assurance as to the integrity and reliability of financial reporting.

In accordance with section 45E of the Public Finance Act 1989, I report as follows.

The financial statements are audited by the Audit Office and their report is attached.



Dr W H Tucker
Director GCSB

25 September 2006



Countersigned by

C B G Carson BCA, CA
Chief Financial Officer

25 September 2006

STATEMENT OF EXPENDITURE AND APPROPRIATION

The total appropriation was \$37.983 million.

The expenditure out-turn on the Vote was \$37.977 million or 0.016% less than the appropriation.

	GST Inc \$000
Total appropriation.....	\$37.983
Actual Expenditure.....	\$37.977

AUDIT REPORT

TO THE READERS OF GOVERNMENT COMMUNICATIONS SECURITY BUREAU'S STATEMENT OF EXPENDITURE AND APPROPRIATION FOR THE YEAR ENDED 30 JUNE 2006

The Auditor-General is the auditor of the Government Communications Security Bureau (the Bureau). The Auditor-General has appointed me, Terry McLaughlin, using the staff and resources of Audit New Zealand, to carry out the audit of the statement of expenditure and appropriation of the Bureau, on his behalf, for the year ended 30 June 2006.

Unqualified Opinion

In our opinion the statement of expenditure and appropriation (the statement) of the Bureau on page 26 fairly reflects the actual expenses and capital expenditure against the Bureau's appropriation for the year ended 30 June 2006.

The audit was completed on 25 September 2006, and is the date at which our opinion is expressed.

The basis of the opinion is explained below. In addition, we outline the responsibilities of the Chief Executive and the Auditor, and explain our independence.

Basis of opinion

We carried out the audit in accordance with the Auditor-General's Auditing Standards, which incorporate the New Zealand Auditing Standards.

We planned and performed the audit to obtain all the information and explanations we considered necessary in order to obtain reasonable assurance that the statement did not have material misstatements, whether caused by fraud or error.

Material misstatements are differences or omissions of amounts and disclosures that would affect a reader's overall understanding of the statement. If we had found material misstatements that were not corrected, we would have referred to them in our opinion.

The audit involved performing procedures to test the information presented in the statement. We assessed the results of those procedures in forming our opinion.

Audit procedures generally include:

- determining whether significant financial and management controls are working and can be relied on to produce complete and accurate data;
- verifying samples of transactions and account balances;
- performing analyses to identify anomalies in the reported data;
- reviewing significant estimates and judgements made by the Chief Executive;
- confirming year-end balances;
- determining whether accounting policies are appropriate and consistently applied; and

- determining whether the statement disclosures are adequate.

We did not examine every transaction, nor do we guarantee complete accuracy of the statement.

We evaluated the overall adequacy of the presentation of information in the statement. We obtained all the information and explanations we required to support our opinion above.

Responsibilities of the Chief Executive and the Auditor

The Chief Executive is responsible for preparing a statement that provides a record of the total of actual expense and capital expenditure incurred for the financial year against the Bureau's appropriation for that financial year. The Chief Executive's responsibilities arise from the Public Finance Act 1989.

We are responsible for expressing an independent opinion on the statement and reporting that opinion to you. This responsibility arises from section 15 of the Public Audit Act 2001 and section 45D (2) of the Public Finance Act 1989.

Independence

When carrying out the audit we followed the independence requirements of the Auditor-General, which incorporate the independence requirements of the Institute of Chartered Accountants of New Zealand.

Other than the audit, we have no relationship with or interests in the Bureau.



Terry McLaughlin
Audit New Zealand
On behalf of the Auditor-General
Wellington, New Zealand

Matters relating to the electronic presentation of the statement of expenditure and appropriation

This audit report relates to the statement of expenditure and appropriation (the statement) of Government Communications Security Bureau (the Bureau) for the year ended 30 June 2006 included on the Bureau's web site. The Bureau's Chief Executive is responsible for the maintenance and integrity of the Bureau's web site. We have not been engaged to report on the integrity of the Bureau's web site. We accept no responsibility for any change that may have occurred to the statement since it was initially presented on the web site.

The audit report refers only to the statement named above. It does not provide an opinion on any other information which may have been hyperlinked to/from that statement. If readers of this report are concerned with the inherent risks arising from electronic data communication they should refer to the published hard copy of the audited statement and related audit report dated 25 September 2006 to confirm the information included in the audited statement presented on this web site.

Legislation in New Zealand governing the preparation and dissemination of financial statements may differ from legislation in other jurisdictions.