



Government Communications Security Bureau

ANNUAL REPORT

for the year ended 30 June 2005

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 2005.

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	2
TABLE OF CONTENTS.....	3
DIRECTOR'S OVERVIEW.....	4
STATEMENT OF PURPOSE.....	6
MISSION AND OUTCOMES.....	7
Mission Statement	7
Vision	7
Outcomes.....	8
ACHIEVEMENT OF OUTCOMES	10
Provision of Intelligence and Threat Warning Information.....	10
Protecting Official Information and the National Critical Information Infrastructure.....	11
Statement on Interception Warrants	13
Statement on Computer Access Authorisations	13
Oversight and Review.....	14
Internal Audit and Intelligence Compliance	14
Legal and Statutory.....	14
ORGANISATIONAL INFORMATION.....	15
Corporate Structure	15
People Capability	16
STATEMENT OF RESPONSIBILITY.....	19
STATEMENT OF EXPENDITURE AND APPROPRIATION	20
AUDIT REPORT	21

Part One

Director's Overview

DIRECTOR'S OVERVIEW

The 2004-05 financial year was a busy one as the Bureau worked to deliver its services to Government and to enhance its capabilities against the backdrop of a growing demand for a widening range of 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 a reorganisation of the Bureau's intelligence production unit and an increase in the number of analysts, continued enhancements to the Bureau's two collection stations at Tangimoana and Waihopai, and advances in a number of other capabilities, to 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 significant focus of the GCSB's operations throughout the year has been the ongoing development of our relationships with key customers, in particular the provision of intelligence and information systems security support and advice to the New Zealand Defence Force (NZDF) and the Ministry of Defence.

The Bureau has 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.

A start was made on the reshaping and enhancement of the information systems security side of the Bureau's business. An internal reorganisation accompanied by an increase in staffing in selected areas, redesigned work processes and the ongoing development of the Centre for Critical Infrastructure Protection are all designed to contribute to an enhanced information systems security service, well placed to meet future Government demands.

Internally, the Bureau continued to implement its Human Resources Strategy, focussing this year on the development of a Bureau-wide Career Development Strategy, fine-tuning the Bureau's individual performance management system, enhancing staff understanding of the performance-based remuneration system, and further developing succession planning within the Bureau.

In the Information and Communications Technology area, a long-term Technology Strategy is being developed, a significant effort continues to address internal IT security and accreditation issues, and the structure and staffing of the Technology Division has been reviewed to ensure that it is best placed to meet Bureau requirements.

This has been a successful year for the Bureau. I look forward to continuing achievement in the year ahead.



Warren Tucker
Director

Part Two

Statement of Purpose

MISSION AND OUTCOMES

Mission Statement

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

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

Vision

“To be the leading source of foreign intelligence and information systems security advice to Government.”

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 person.

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 national critical infrastructure.

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

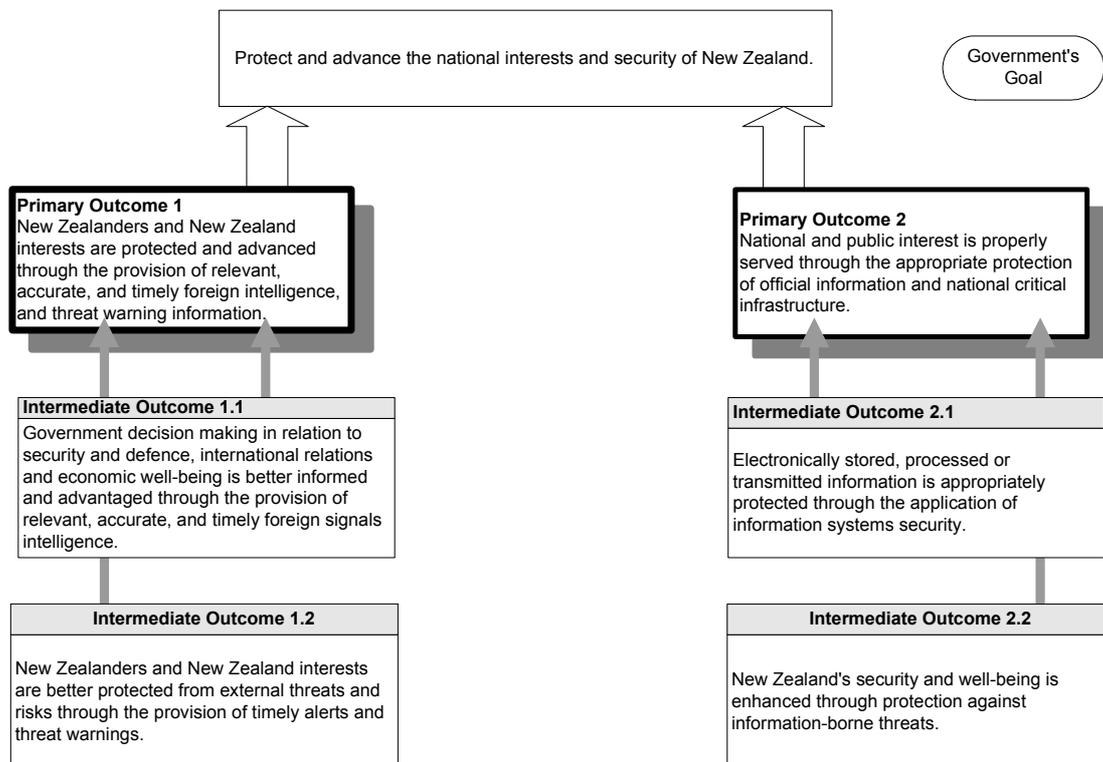


Figure 1 – GCSB Outcomes

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 increased intelligence production during the year, which included a significant effort on counter-terrorism, is directly attributable to an increase in production staff during the reporting year.

A major focus throughout the year was on increasing the level of intelligence support to other Government departments.

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 a week 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 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 National Critical Information Infrastructure

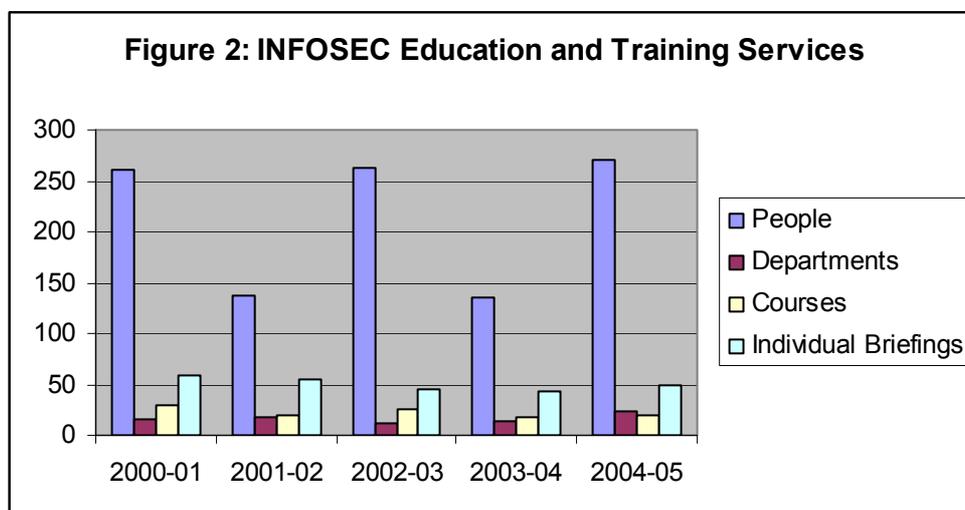
“National and public interest is properly served through the appropriate protection of official information and national critical information infrastructure.”

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 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 services continued to grow during the year. Training and education services have been reinstated after a hiatus during the second half of the previous year due to staff shortages. This is illustrated in Figure 2 below, with numbers increasing in all areas, and the number of individuals provided with advice and assistance exceeding the FY2002-03 levels. 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.



During FY2004-05, the Bureau conducted 19 training courses involving 271 personnel representing 23 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 national critical information 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 957 alerts and advisories, from a wide variety of sources. Eight CCIP newsletters were also published to customer organisations.

The CCIP also designed and issued a CCIP Incident Reporting card, which assists critical information infrastructure organisations in reporting and managing the initial stages of a cyber incident, and published three detailed research papers on Radio Frequency Identification, Voice over Internet Protocol (VoIP) background, and VoIP Security.

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 2005.

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 2005.

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. 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 and Intelligence Compliance

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. The reviews conducted were a Payroll Review, a Capital Expenditure Review and a Budgeting and Planning Review. PriceWaterhouseCoopers also carried out a follow up of the FY2003-04 review recommendations.

During the financial year the position of Intelligence Compliance Manager was established. The primary role of the Intelligence Compliance Manager is to complement the statutory oversight functions of the Inspector-General of Intelligence and Security by ensuring that the Signals Intelligence activities of the GCSB comply with the law and the internal rules governing the production of foreign intelligence by the Bureau.

Legal and Statutory

The Bureau maintains a small legal 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 five functional areas:

- Intelligence Collection and Processing;
- Intelligence Production and Customer Services;
- 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:

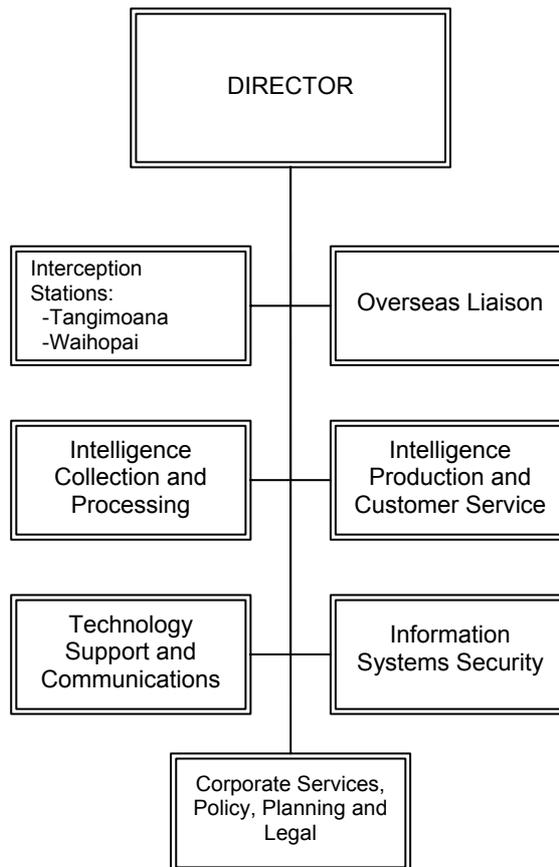


Figure 3 – GCSB Organisation

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 continued to progress implementation of its Human Resources strategy, which is designed to provide it with the flexible, innovative workforce that is required to support its mission. A particular focus during the year has been the development of a Bureau-wide Career Development Strategy which focuses on the ongoing career development and succession planning of employees within the Bureau. Other priorities have been further enhancements to staff training and development, and a second formal succession planning group created to ‘groom’ staff for potential unit managerial and expert roles in the future.

Considerable effort was made during the year to further develop the Bureau’s individual performance management system and to align it more closely with our remuneration practice.

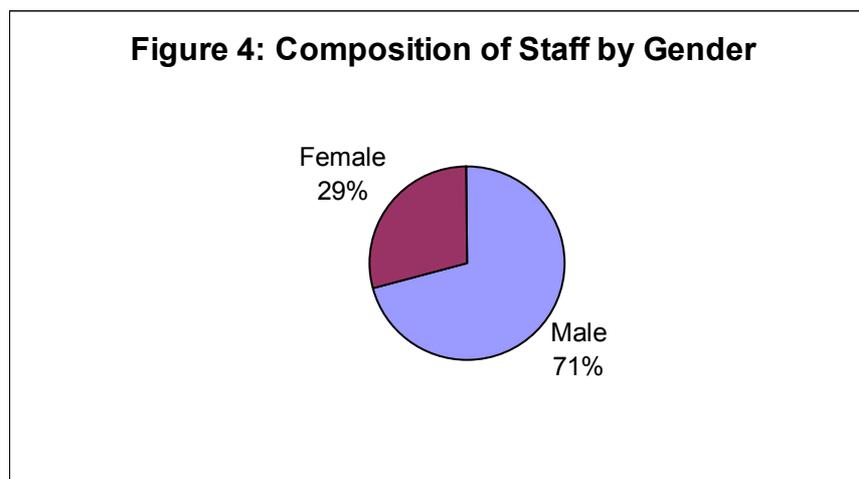
Encouraging Diversity within the GCSB

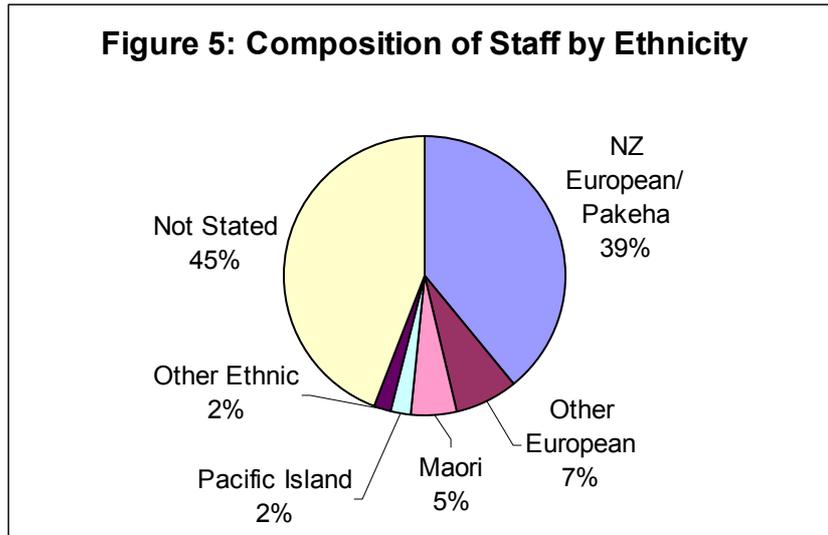
The Bureau recognises that understanding and knowledge of different perspectives enhances the performance of its employees and hence the organisation. In addition to complying fully with the Human Rights Act 1993, and the New Zealand Bill of Rights Act 1990, we are endeavouring to achieve this through:

- 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.





Operational Capacity – Staffing Numbers

The total number of staff employed in the GCSB at 30 June 2005 was 329, an 8.5% increase compared to total staff employed at 30 June 2004. Staff turnover (excluding fixed term and casual employees) decreased from 4.4% last year to 3.9%. Staff turnover was evenly distributed on a proportional basis across the Bureau.

Leadership Development

The Bureau continues to make a particular effort in terms of developing its internal leadership succession policy, with the establishment of two groups, a Leadership Succession Group consisting of Tier 3 Managers considered to have the potential for future Tier 2 roles, and a Leadership Development Group made up of more junior staff assessed as having the potential for future Tier 3 roles (and beyond). Dedicated funding has now been provided to meet the training and development needs of both groups.

Accommodation

As a consequence of increasing staff numbers, the Bureau acquired additional office space in Wellington during the year.

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

29 September 2005



Countersigned by

C B G Carson BCA, CA
Chief Financial Officer

29 September 2005

STATEMENT OF EXPENDITURE AND APPROPRIATION

The total appropriation was \$38.963 million.

The expenditure out-turn on the Vote was \$38.963 million or 100 per cent of appropriation.

	GST Inc \$000
Total appropriation.....	\$38,963
Actual Expenditure.....	\$38,963



AUDIT REPORT

AUDIT REPORT

TO THE READERS OF THE GOVERNMENT COMMUNICATIONS SECURITY BUREAU'S FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2005

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 financial statements of the Bureau, on his behalf, for the year ended 30 June 2005.

Unqualified Opinion

In our opinion the financial statements of the Bureau:

- σ comply with generally accepted accounting practice in New Zealand; and
- σ fairly reflect:
 - the Bureau's financial position as at 30 June 2005; and
 - the results of its operations and cash flows for the year ended on that date.

The audit was completed on 29 September 2005, and is the date at which our opinion is expressed.

The basis of our 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 financial statements 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 financial statements. 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 financial statements. We assessed the results of those procedures in forming our opinion.

Audit procedures generally include:

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

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

We evaluated the overall adequacy of the presentation of information in the financial statements. 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 financial statements in accordance with generally accepted accounting practice in New Zealand. Those financial statements must fairly reflect the financial position of the Bureau as at 30 June 2005. They must also fairly reflect the results of its operations and cash for the year ended on that date. The Chief Executive's responsibilities arise from the Public Finance Act 1989.

We are responsible for expressing an independent opinion on the financial statements and reporting that opinion to you. This responsibility arises from section 15 of the Public Audit Act 2001 and 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
On behalf of the Auditor-General
Wellington, New Zealand

Matters relating to the electronic presentation of the audited financial statements

This audit report relates to the financial statements of the Government Communications Security Bureau (the Bureau) for the year ended 30 June 2005 included on the Bureau's website. The Chief Executive is responsible for the maintenance and integrity of the Bureau's website. We have not been engaged to report on the integrity of the Bureau's web site. We accept no responsibility for any changes that may have occurred to the financial statements since they were initially presented on the web site.

We have not been engaged to report on any other electronic versions of the Bureau's financial statements, and accept no responsibility for any changes that may have occurred to electronic versions of the financial statements published on other websites and/or published by other electronic means.

The audit report refers only to the financial statements named above. It does not provide an opinion on any other information which may have been hyperlinked to/from these financial statements. 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 financial statements and related audit report dated 29 September 2005 to confirm the information included in the audited financial statements presented on this web site.

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