

APPENDIX A

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga



8 May 2006

David Shanks
Chief Legal Advisor
State Services Commission
100 Molesworth St
WELLINGTON

Dear Mr Shanks

State Services Commission Inquiry into disclosure of classified information about the Government's Telecommunications Stocktake Review to Telecom – Appointment under section 25(2) State Sector Act 1988

You are aware that I am undertaking an investigation into the above matter. In undertaking this investigation, I am carrying out my functions under sections 6(b) and 57B of the State Sector Act 1988. The Minister of State Services has also agreed Terms of Reference for me to undertake this inquiry. These Terms of Reference require me to:

- investigate how Telecom came to possess classified information about the Government's Telecommunications Stocktake Review;
- report to the Prime Minister and the Minister of State Services on the outcome of the investigation.

I specifically appoint you to conduct the investigation and to report to me on your findings. Such appointment is in terms of section 25 of the State Sector Act 1988, and accordingly the powers and authority conferred on me by section 25(1) of that Act shall attach to and be exercised by you in undertaking the investigation, pursuant to section 25(2).

For the avoidance of doubt, your appointment to conduct the investigation shall not prevent me from appointing additional persons to conduct the investigation as may be required.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Mark Prebble'.

Mark Prebble
State Services Commissioner

APPENDIX B



Office of Hon Annette King, M.P.

Minister of State Services

Minister of Police

Minister for Food Safety

MP for Rongotai (incl. Chatham Islands)

Associate Minister of Defence

Associate Minister of Trade

Co-ordinating Minister, Race Relations

9 May 2006

Dr Mark Prebble
State Services Commissioner
State Services Commission
PO Box 329
Wellington

Dear Mark,

Investigation into unauthorised disclosure of classified information

This note confirms my oral instructions to you last Wednesday, 3 May 2006.

In accordance with section 8 of the State Sector Act 1988, I am directing you to conduct an investigation into the unauthorised disclosure of information regarding the Telecommunications Stocktake Review to Telecom New Zealand last week.

I attach terms of reference for the investigation, which have been discussed with you.

Yours sincerely,

A handwritten signature in cursive script, appearing to read 'Annette King'.

Hon Annette King
Minister of State Services

Investigation into disclosure of classified information about the Government's Telecommunications Stocktake Review to Telecom

Terms of reference

The Minister of State Services has directed the State Services Commissioner, Mark Prebble, pursuant to provisions of the State Sector Act 1988, to investigate how classified information about the Government's Telecommunications Stocktake Review came into the possession of Telecom New Zealand.

Information about the Telecommunications Stocktake Review was contained in classified Cabinet documents, which were distributed in accordance with the Cabinet Office's standard distribution procedures for classified documents of this nature.

The Government takes the unauthorised disclosure of Cabinet documents, or the information contained in such documents, very seriously. The Prime Minister has determined that an investigation should be held to ascertain how Telecom came to possess classified information about the Government's Telecommunications Stocktake Review.

The State Services Commissioner will:

- investigate how Telecom came to possess classified information about the Government's Telecommunications Stocktake Review; and
- report to the Prime Minister and the Minister of State Services on the outcome of the investigation.

APPENDIX C



MARK VERBIEST
Group General Counsel

Telecom New Zealand Limited
Telecom House
68-86 Jervois Quay
P O Box 570
Wellington

5 May 2006

Dr Mark Prebble
State Services Commissioner
100 Molesworth Street
WELLINGTON

COMMERCIAL IN CONFIDENCE

Dear Dr Prebble

Re: Telecommunications Stocktake

We understand that the State Services Commission intends to conduct an investigation into a document provided to Telecom in relation to the Telecommunications Stocktake.

The purpose of this letter is to advise you as to the findings of Telecom's own investigation into the circumstances in which the document came into our hands.

Our understanding of what took place is as follows:

- The person who gave the document to a Telecom employee ("Telecom Employee") was a Parliamentary Messenger named Mike Ryan.
- Mr Ryan and the Telecom Employee, and their families, have been friends for some 15 years. They are part of common social groups.
- On the evening of Monday 1 May, Mr Ryan came to the Telecom Employee's home to look at carpet which was to be removed and which Mr Ryan may have been able to use. In the course of this visit, Mr Ryan mentioned, without prompting and out of context, that a paper concerning telecommunications was going to be presented to Cabinet on the upcoming Wednesday. Mr Ryan mentioned that the paper recommended "doing something with the local loop". The Telecom Employee felt uncomfortable with these comments and changed the topic of conversation. The matter was not raised again. The Telecom Employee and Mr Ryan had not had a conversation along these lines at any time / previously or subsequently.
- On the evening of Tuesday 2 May, Mr Ryan, the Telecom Employee, and others attended a meeting to discuss a fundraising event being organised by a sporting group to which Mr Ryan and the Telecom Employee

Telecom New Zealand Limited

Telecom House • 68 Jervois Quay • PO Box 570 Wellington New Zealand
Telephone 64-4-498 9054 • Fax 64-4-499 6524 • Email markverbiest@telecom.co.nz

belonged. The meeting was held at the home of another member of the group and concluded at approximately 10:45pm.

- After the meeting, Mr Ryan, Mr Ryan's wife, the Telecom employee and another person walked to Mr Ryan's car. Just before getting into the car, Mr Ryan handed a manila folder to the Telecom Employee. Mr Ryan did not say what the manila folder contained but told the Telecom Employee that it might be of interest. He asked the Telecom Employee not to copy it, and to return it the next morning.
- After being dropped home, the Telecom Employee scanned the first one or two pages of the document but did not read the contents in detail. The Telecom Employee took a copy of the document that evening.
- At approximately 7:30am, Wednesday 3 May, the Telecom Employee went to the home of Mr Ryan and returned the manila folder and the original document without discussion.
- After returning home, the Telecom Employee travelled to the office. The Telecom Employee wished to seek advice as to what to do with the copy of the document and his first action that morning was to make contact with one of Telecom's in-house lawyers. The Telecom Employee consulted with that lawyer at approximately 9.45am and delivered the copy of the document to that lawyer.
- After considering the document, Telecom formed the view that it could potentially give rise to disclosure obligations under the NZX and ASX listing rules. Telecom sought urgent clarification of the document's status from Mr Cunliffe's office and from the Office of the Prime Minister.
- As you will be aware, at 4:30pm, it was announced that the Minister would hold a media conference at 5:15pm for the purposes of making an announcement of the Government's decision on this matter. Telecom became aware of this announcement between 4.45pm and 5.00pm.
- The investigation has concluded that:
 - the Telecom Employee has not received confidential information from Mr Ryan on any other occasion;
 - the Telecom Employee did not solicit confidential information from Mr Ryan; and
 - Mr Ryan provided this information out of a misguided sense of friendship.

The employee who originally received the document has co-operated fully with our inquiry and returned early from an overseas business trip so that they could be interviewed in person this morning. The employee also naturally has concerns about having had to name a longstanding personal friend who provided the document, although that friend appears to have made a grave error of judgment.

Yours sincerely



Mark Verbiest
Group General Counsel

Telecom New Zealand Limited

Telecom House • 68 Jervois Quay • PO Box 570 Wellington New Zealand
Telephone 64-4-498 9054 • Fax 64-4-499 6524 • Email markverbiest@telecom.co.nz

APPENDIX D



Department of the Prime Minister & Cabinet

Declaration of Confidentiality

I, _____

shall be discreet in all matters relating to Department of the Prime Minister & Cabinet (DPMC) affairs and the affairs of the New Zealand Government.

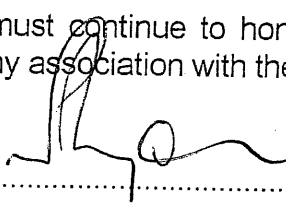
Information obtained through my employment/engagement with the DPMC shall not be disclosed to or discussed with any person who is not entitled to the information, nor shall I use such information to gain personal material advantage or financial benefit for any other person or organisation. This restriction shall operate until such information is publicly available or until the DPMC gives approval to its disclosure or use.

I shall not state, indicate or otherwise purport to be an agent or representative of the DPMC, or cause any other person to believe that I am an agent or representative of the DPMC unless prior consent in writing has been given by the DPMC.

I promise to maintain confidentiality in respect of all matters that may come to my knowledge in the course of my employment with the DPMC.

I promise never to disclose any information from the DPMC to anyone except when performing my duties or required by law.

I acknowledge that I must continue to honour these promises I make in signing this document, even after my association with the DPMC has ceased.

Signature: 

Place: Wellington

Date: 20.10.05

Witness: Rachel Goodfellow Roopler

APPENDIX E

Information Systems Code of Practice Agreement

In the event that you are found to have seriously breached any or all of these policies then this will be regarded as serious misconduct and may result in dismissal. If the breach is considered less serious, you will be warned that an ongoing breach of any of the policies may result in your dismissal.

INFORMATION SYSTEMS

DPMC acknowledges that optimal staff performance requires the use of modern technology and information systems.

DPMC agrees:

- To provide me with any appropriate computer equipment, electronic communications system, document management system, and information systems necessary for me to carry out my job in an efficient and effective manner.

I understand and agree that:

- I have read the "Information Systems Code of Practice" and will abide by the principles outlined.
- I have read the Internet and Email policies and will abide by the principles outlined.
- I will not misuse any systems provided.
- I will not knowingly do anything that brings down the system or causes unnecessary congestion to the system.
- I will not breach confidentiality.
- I will not, knowingly, expose the department to risk or bring the department into disrepute.
- I will not access inappropriate or objectionable material.
- My system activities will be routinely monitored by the department.
- I will not share my system password with anyone.
- I will not disclose any technical information concerning DPMC information systems to anyone outside of DPMC without prior agreement with Corporate Services, nor in the case of a business unit information system, without approval from the business unit system administrator.
- I will comply with any requests and advice given to me, from time to time, in relation to the use of technology in the department.
- Access to my computer equipment and logins will only be given when there is a business reason.

HEALTH AND SAFETY

DPMC endorses the good employer provisions of the State Sector Act. DPMC accepts that there are health considerations relating to the use of computer equipment and is aware of the long term effects of Occupational Overuse Syndrome on staff health.

DPMC agrees:

- To provide information about the safe use of computer equipment to all staff.
- To ensure that a workstation assessment is completed for all DPMC staff who use computer equipment.
- To provide appropriate equipment for the safe use of information systems.
- To provide software to minimise, manage, monitor, and report any possible overuse health hazard relating to the use of the computer.

I Understand and agree:

- To read and act upon all the material provided by DPMC on the safe use of computer equipment.
- To contact Corporate Services if I need further advice on health and safety issues regarding the safe use of computer equipment.
- To let my manager know if I suffer from, or have suffered from, a pre-existing condition that could recur or be worsened by using a computer.
- To advise Corporate Services and my manager if the use of computer equipment results in an injury, whether or not this injury results in Occupational Overuse Syndrome.
- To allow the department to monitor my computer usage and work practices for the purposes of minimising any potential hazard.

I, Michael Patrick Ryan have read this code of practice and agree to abide by the guidelines and conditions set out in this document.

Signed 

Date 22/12/05

Approved by SMG – December 2004

APPENDIX F

Confidentiality Maintaining the integrity and security of official information is a vital issue for DPMC. Departmental staff are privy to a wide range of information and advice that you may see or hear in the course of their duties.

For this reason, on joining the department you are required to agree and sign a Declaration of Confidentiality.

At all times, you must exercise discretion in dealing with DPMC matters and must treat with care any information to which they have access. In particular information gained in the course of official duties must not be used:

- In ways that would undermine impartiality
- To allow a member of staff or other person gain an improper advantage

The unauthorised use or disclosure (leaking), by DPMC staff (including secondees and contractors), of information to which they have had official access, will result in disciplinary action that may include dismissal. This confidentiality requirement continues even after you cease your employment or involvement with DPMC.

Classified Information Many staff in DPMC have access to classified documents. The principles relating to confidentiality (set out above) also apply to classified information. In addition, there are also special rules and handling requirements (see the manual "Security in Government Departments" and other relevant instructions).

Specific guidance is issued to staff on handling classified documents. Failure to observe relevant security procedures is a serious lapse of duty.

APPENDIX G

Release of Official Information

The disclosure of official information is subject to the requirements of the Official Information Act 1982. The general principle of the Act is that information should be made available on request, unless compelling reasons exist why it should not. These reasons are detailed in the Act.

Departments may establish specific procedures for dealing with the release of information provided they do not conflict with those of the Act. Official information should be released only in accordance with those procedures and by public servants authorised to deal with requests for information. In all other circumstances, information is to be used by public servants only for official purposes and treated as confidential to the department.

Public servants authorised by their department to respond to requests made under the Official Information Act should exercise proper care and discretion in the application of departmental procedures. In cases of doubt, public servants should seek guidance from departmental legal advisers. Should the release of politically sensitive material be required, public servants should ensure that the Minister is notified well in advance of any information release.

It is unacceptable for public servants to make unauthorised use or disclosure of information to which they have had official access. Whatever their motives, such employees betray the trust put in them, and undermine the relationship that should exist between Ministers and the Public Service. Depending on the circumstances of the case, the unauthorised disclosure of information may lead to disciplinary action, including dismissal.

APPENDIX H

Annex B—Management of Material Classified as SENSITIVE

SENSITIVE	Compromise of information would be likely to damage the interests of New Zealand or endanger the safety of its citizens.
Guidelines:	<ul style="list-style-type: none"> • Endanger the safety of any person. • Damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to: <ul style="list-style-type: none"> – exchange rates or the control of overseas exchange transactions – the regulation of banking or credit – taxation – the stability, control, and adjustment of prices of goods and services, rents and other costs, and rates of wages, salaries and other incomes – the borrowing of money by the Government of New Zealand – the entering into of overseas trade agreements. • Impede a Minister of the Crown or a department organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations).
Principles and Clearance Levels	<ul style="list-style-type: none"> • Information classified as SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the department to access SENSITIVE level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	<ul style="list-style-type: none"> • All SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by the GCSB.
Electronic Storage	<ul style="list-style-type: none"> • Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: <ul style="list-style-type: none"> – user challenge and authentication (username/password or digital ID/Certificate) – logging use at level of individual – firewalls and intrusion-detection systems and procedures; server authentication – OS-specific/application-specific security measures.

Electronic Disposal	<ul style="list-style-type: none"> • Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Manual Transmission	<ul style="list-style-type: none"> • Within a single physical location. As determined by the Chief Executive or Head of the organisation. • Transfer between establishments within or outside New Zealand. <ul style="list-style-type: none"> – May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word SENSITIVE is not visible. – The outer envelope should be addressed to an individual by name and title. SENSITIVE mail for/from overseas posts should be carried by diplomatic airfreight through MFAT. – The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.
Manual Storage	<ul style="list-style-type: none"> • In an office environment, SENSITIVE material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	<ul style="list-style-type: none"> • Disposed of or destroyed in a way that makes reconstruction highly unlikely.