STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

6 July 2018

[redacted]

Dear [redacted]

Official information request

Our ref: SSC2018/0102

I refer to your official information request received on 26 June 2018 for:

> *"Copy of the 2000 Cabinet document/decision on security. Classifications: CAB (00) M42/4G (4) and any associated documents from that time provided with CAB (00) M42/4G (4). The Cabinet paper was taken to Cabinet by the SSC minister."*

Information being released

Please find enclosed the following documents in response to your request:

Item	Document Description	Decision
1	10 November 2000 Briefing Paper – Protection of Official Information	Released in full
2	CAB (00) M 42/4G(4)	Released in full

If you wish to discuss this decision with us, please feel free to contact Ministerial.Services@ssc.govt.nz.

Please note that we intend to publish this letter (with your personal details removed) [and enclosed documents] on the State Services Commission's website.

Yours sincerely

Stephen Moore
Managing Principal
State Services Commission

2 The Terrace
PO Box 329 Wellington 6140
New Zealand
Phone +64-4-495 6600
Fax +64-4-495 6686
www.ssc.govt.nz

Submission Cover Sheet

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

> Unclassified
> In Confidence
> Sensitive
> Restricted
>

Date: 10 November 2000

Submission Number: 11/00-MoSS/AMoSS/171

Sensitivity:

Output Number:

Submission Type: Briefing Paper

Subject: Protection of Official Information

Recipient	Action Sought	Deadline
MoSS and AMoSS	Note and agree with recommendation in briefing paper.	
Copies to:		

Contact for Telephone Discussion (if required)

Name:	Role:	Telephone		Suggested First Contact
		Direct	After Hours	
Hugh McPhail	Team Manager	495 6688		1

Minister's Office to Complete

☐ Noted ☐ Seen ☐ Approved

☐ Needs Change ☐ Referred to ----------

☐ Withdrawn ☐ Not seen by Minister ☐ Overtaken by events

Comment

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

10 November 2000

Minister of State Services
Associate Minister of State Services

PROTECTION OF OFFICIAL INFORMATION

Purpose

1 This note outlines the proposed framework for the protection of official information that has been developed by the Interdepartmental Committee on Security, and the process proposed for its adoption and implementation.

Background

2 The main purpose of the Official Information Act 1982 is to make official information readily available to the public unless there are good reasons for withholding it. Another purpose is to protect official information to the extent consistent with the public interest and the preservation of personal privacy. The Act provides reasons for withholding information and where information is withheld allows for it to be protected.

3 The present system for protecting official information was instituted by Cabinet in 1982 (CM 82/52/24 refers). As a result, DPMC and SSC have jointly led a process to identify these deficiencies and how they should be overcome.

4 The system approved in 1982 provides three classifications, TOP SECRET, SECRET and CONFIDENTIAL. These classifications are used to grade information on the basis of content and the damage to national security that would result from unauthorised disclosure, and to specify the protective measures to be applied. The rules provided are mainly applicable to departments who hold information of a national security nature such as the Ministry of Foreign Affairs and Trade, the Ministry of Defence, the New Zealand Defence Force, the Department of the Prime Minister and Cabinet, the intelligence agencies, and occasionally other agencies such as the Treasury and Police.

Problems With Current System

5 Most government departments and agencies seldom, if ever, hold information that requires protection for reasons of national security. Rather, the information needs protection from unauthorised disclosure for motives such as avoiding the premature disclosure of government decision-making, complying with personal privacy requirements or protecting commercially sensitive material. The present system does not administer this situation adequately and the lack of relevant rules has led to individual departments developing practices without sufficient consideration of how these might work in the wider state sector. The resulting arrangements are ad hoc, lack any overall consistency or coherence and create uncertainty as to the level of protection required in handling information in many instances. Uniform standards will be required to enable departments to share information and be confident that it will be appropriately protected wherever it is held.

100 Molesworth Street
PO Box 329 Wellington
New Zealand
Phone +64-4-495 6600
Fax +64-4-472 5979
www.ssc.govt.nz

6 The 1982 review provided rules for a predominantly paper environment. The rules have subsequently been updated to protect information held in national security computer systems. But, they do not particularly suit a world where information of an administrative nature is increasingly being stored and transferred electronically. What is needed are some sensible rules that provide a suitable level of protection for computer systems without requiring the high-grade protective devices, the demanding physical access controls and the higher compliance costs associated with national security systems. This situation has been highlighted by developments such as:

7 Improved electronic security is one of the foundations of the e-government programme. Citizens will expect information they provide within this umbrella to be afforded consistent protection from unauthorised disclosure during transmission, in storage and when being finally disposed of. The deficiencies in the present system must be overcome before e-government initiatives can be implemented effectively.

8 A pilot project involving the Department of Prime Minister and Cabinet, the State Services Commission and the Treasury looked at approaches to creating a secure electronic environment (SEE) enabling those agencies to exchange e-mail and access databases of electronic information held by participating departments. Once proven, it is intended that this secure system be made available to other government departments.

9 At the bottom end there is a straight choice between classifying material CONFIDENTIAL and treating it as unclassified with no protection at all; as a result CONFIDENTIAL is often used by some agencies because there is no intermediate classification available. The result is that large volumes of information are unnecessarily processed within systems embodying high-grade encryption; this is a problem particularly experienced within the overseas cable system of the Ministry of Foreign Affairs and Trade.

10 The present system does not mesh well with those of our overseas partners, particularly Australia. They have an intermediate classification RESTRICTED that creates a difficulty for departments such as the Ministry of Foreign Affairs and Trade and the Defence Force, who upgrade such material to CONFIDENTIAL so that a level of protection at least as good as that expected by their overseas counterparts is assured.

Proposed Framework

11 The Interdepartmental Security Committee (ICS), chaired by the Director of the Domestic and External Security Secretariat in DPMC, has been working to produce a revised system that suits the New Zealand situation. The objective is to be flexible so that the needs across all government agencies are met and an appropriate balance is set between protecting official information and the compliance costs of the protective measures.

12 The approach now being proposed is to introduce a separate framework for administering information that requires protection for reasons other than national security; i.e. the system used by Australia. The advantage of two separate frameworks is that they avoid any potential for conflict between the very specific requirements of the national security environment and the risk management approach that is more relevant

for protecting other types of official information. This approach has found most favour amongst government departments.

13 The proposed approach would introduce a new framework for administrative information with two security classifications SENSITIVE and IN CONFIDENCE (investigation shows that two classifications will provide a framework with sufficient flexibility; a single classification would lead to over-protection in many instances whereas more than two would make the framework unnecessarily complex). The system would preserve the existing framework of TOP SECRET, SECRET and CONFIDENTIAL used for national security information and add a further security classification of RESTRICTED.

14 The protective measures for handling information classified as TOP SECRET, SECRET and CONFIDENTIAL will be unchanged; these rules are set explicitly with little or no discretion allowed in their application. The guidelines covering RESTRICTED are new. All four sets of guidelines are similar to those in use by Australia. A more flexible approach will be adopted for RESTRICTED, SENSITIVE and IN CONFIDENCE, with protective measures being tailored to specific situations. In these instances, chief executives will be responsible for setting the levels of protection to be applied within their departments. A risk management approach will be used to achieve a relevant level of protection as cost-effectively as possible, but taking into account a minimum level to be observed across all departments. The Cabinet paper will set out proposed guidelines for protecting RESTRICTED, SENSITIVE and IN CONFIDENCE information. These guidelines will cover information held in paper or electronic form. Common guidelines will apply to RESTRICTED and SENSITIVE information, whereas the rules for IN CONFIDENCE are less onerous.

Official Information Act

15 The Official Information Act 1982 allows information to be protected to the extent consistent with the public interest and the preservation of personal privacy. Classifications are used to grade information on the basis of content and the damage that would result from unauthorised disclosure, and to specify the protective measures to be applied. In themselves, classifications do not allow official information to be withheld; rather, the content must be considered on its merits using the criteria in the Act.

Consultation

16 The process has involved extensive consultation. In the initial stage MFAT, Treasury, Cabinet Office, Police, DWI, IRD, NZDF, GCSB, NZSIS, GOVIS, the Ombudsman and the Privacy Commissioner were consulted. Further consultation now includes all of the remaining departments of the Public Service. It is currently envisaged that a paper will be submitted to the Cabinet Committee on Government Expenditure and Administration (EXG) for its meeting on 29 November 2000, and will be co-signed by the Prime Minister and the Minister of State Services.

Implementation

17 Subject to Cabinet endorsement, the new system will be implemented over a two-year period starting in February 2001. During year one the State Services Commission and the Department of Prime Minister and Cabinet will arrange a training programme for

security officers in all government departments. In year two the State Services Commission will institute an audit programme to confirm compliance with the new system.

18 The manual, *Security in Government Departments,* will be re-issued. The State Services Commission will be responsible for manual content covering information requiring protection for public interest and personal privacy reasons and the Department of Prime Minister and Cabinet for that associated with national security.

19 The proposed system has been developed for use by government departments and within ministerial offices. It will also be made available to state owned enterprises and Crown entities to assist them in meeting their obligations under the Official Information Act 1982 and the Privacy Act 1993.

Comment

20 The Commission believes that the proposed framework will provide a valuable basis for ensuring that information is effectively and consistently protected across the State sector, and is necessary to support the development of e-government initiatives.

21 In view of the implications for e-government and information sharing within the government, a copy of this note is attached for forwarding to the Minister of Information Technology, if you agree.

Recommendations

22 It is recommended that you:

a **note** that officials are preparing a draft paper for EXG proposing a new framework for the classification and protection of official information;

b **note** that the draft paper is currently the subject of consultation with departments;

c **note** that it is envisaged that the Minister of State Services should co-sign the paper with the Prime Minister;

d **agree** that a copy of this briefing should be forwarded to the Minister of Information Technology.

Agree/Disagree

Iona Holsted
for State Services Commissioner

CABINET

CAB (00) M 42/4G(4)

Minister of State Services

CABINET MINUTE NOTED
Commissioner: _____
Deputy Commissioner SSC: _____
Deputy Commissioner: _____
Legal Branch: _____

COPIES TO:

Prime Minister
Deputy Prime Minister
All Ministers
All Chief Executives
Speaker of the House
Chair Parliamentary Service Commission
Controller and Auditor-General
Chief Parliamentary Counsel
Secretary of the Cabinet
Secretary, EXG

Protection of Official Information

All Branch Managers

Reference: CAB (00) 843; EXG (00) M 20/7

At the meeting on 18 December 2000, following reference from the Cabinet Committee on Government Expenditure and Administration, Cabinet:

a **noted** that the system for protecting official information was last reviewed by Cabinet in 1982;

b **noted** that the present system has a number of deficiencies:

i it provides rules that are mainly applicable to official information that requires protection for national security reasons, but does not adequately cover information that needs protection for other reasons, such as preserving personal privacy or avoiding the premature disclosure of government decision-making;

ii it operates effectively in a paper environment, but less so in a world where information is increasingly being held and transferred electronically;

iii it leads to over-classification of official information and expenditure on protective measures greater than warranted;

c **agreed** that these deficiencies can be overcome by a revised system that:

i introduces a new framework for official information requiring protection for public interest and personal privacy reasons with security classifications of SENSITIVE and IN CONFIDENCE:

ii preserves the existing security classifications of TOP SECRET, SECRET and CONFIDENTIAL for information associated with national security, and adds a further classification of RESTRICTED;

d **noted** that the revised system for protecting official information will be consistent with, and not replace, the obligations contained in the Official Information Act 1982;

e **agreed** that the revised system be introduced within government departments, ministerial offices, the NZ Police, the NZ Defence Force, the NZ Security Intelligence Service and the Government Communications Security Bureau, and also be made available to state owned enterprises and crown entities;

f **agreed** that the guidelines for grading information as SENSITIVE, IN CONFIDENCE, TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED be as shown in Annex 1 to this minute;

g **agreed** that chief executives will be responsible for setting the levels of protection for RESTRICTED, SENSITIVE and IN CONFIDENCE information using a risk management approach and taking into account a minimum level to be applied across all departments, as shown in the guidelines attached as Annex 2 to this minute;

h **directed** the State Services Commission and the Department of Prime Minister and Cabinet to coordinate the implementation of the revised system, including the reissue of the manual *Security in Government Departments,* to reflect the above policy;

i **agreed** that a Cabinet Office circular be issued to advise ministerial offices and departments of the implementation of the new requirements in relation to the submission of papers for Cabinet;

j **noted** that implementation of the revised system will occur over a two year period commencing in February 2001;

k **noted** that the costs incurred in implementing the revised system will be accommodated within existing baselines.

Secretary of the Cabinet

PROTECTION OF OFFICIAL INFORMATION

SECURITY CLASSIFICATIONS

INTRODUCTION

This Appendix provides guidelines for selecting an appropriate security classification where it has been determined that official information requires protection using specific handling rules. It is emphasised that the guidelines are not prescriptive; rather they are provided to assist in the classification process. **The classification will be chosen by the responsible departmental staff member through reference to content and the degree of damage or prejudice that would arise from disclosure of the information.**

The two new classifications, **SENSITIVE** and **IN CONFIDENCE**, cover information requiring protection for public interest and personal privacy reasons. Guidelines for grading information as **SENSITIVE** or **IN CONFIDENCE** draw on the reasons in the Official Information Act 1982 for withholding official information.

The three existing classifications **TOP SECRET, SECRET, CONFIDENTIAL,** and a new classification **RESTRICTED** cover information requiring protection for national security reasons; that is situations where making information available would be likely to:

- prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand
- prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the government of any other country, or any agency of a such a government, or any international organisation

Guidelines for grading information as **TOP SECRET, SECRET** or **CONFIDENTIAL** are in essence unchanged, although they have been made more explicit to assist in their application. The guidelines covering **RESTRICTED** are new. All of these guidelines are similar to those in use by Australia.

IMPORTANT NOTE

The Official Information Act allows information to be protected to the extent consistent with the public interest and the preservation of personal privacy.

Classifications are used to grade information on the basis of the damage that would result from unauthorised disclosure and to specify the protective measures to be applied.

In themselves, classifications do not allow official information to be withheld; rather, the information must be considered on its merits using the criteria in the Act.

GUIDELINES FOR SENSITIVE AND IN CONFIDENCE

The following guidelines are for grading information as SENSITIVE or IN CONFIDENCE.

Most information will be adequately protected by the classification IN CONFIDENCE.

Some information will warrant the higher classification SENSITIVE through reference to content and the degree of damage or prejudice that would arise from its disclosure.

SENSITIVE	Compromise of information would be likely to damage the interests of the New Zealand government or endanger the safety of its citizens

Any information that meets the following guidelines will usually be classified as SENSITIVE. In addition, any information covered by the guidelines for IN CONFIDENCE (see next page) should be classified as SENSITIVE, where a determination by subject matter and degree of damage or prejudice that would arise from its disclosure indicates that a greater level of protection is warranted.

- 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:
  - 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 an Department or organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)

IN CONFIDENCE	Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens

Any information that meets the following guidelines will usually be classified IN CONFIDENCE unless a determination by subject matter and degree of damage or prejudice that would arise from its disclosure indicates that a greater level of protection is warranted. If so, the higher classification SENSITIVE should be used.

- prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial
- affect adversely the privacy of natural persons, including that of deceased natural persons
- disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information
- disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would:
  - be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied
  - be likely otherwise to damage the public interest
- prejudice measures protecting the health or safety of members of the public
- prejudice the substantial economic interests of New Zealand
- prejudice measures that prevent or mitigate material loss to members of the public
- breach the constitutional conventions for the time being which protect:
  - the confidentiality of communications by or with the Sovereign or her representative
  - collective and individual ministerial responsibility
  - the political neutrality of officials
  - the confidentiality of advice tendered by Ministers of the Crown and officials
- impede the effective conduct of public affairs through:
  - the free and frank expression of opinions by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty
  - the protection of such Ministers, officers and employees from improper pressure or harassment
- breach legal professional privilege
- impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities
- lead to the disclosure or use of official information for improper gain or advantage

- *NB: Information held internally by a department that is classified as IN CONFIDENCE may not always be labelled as such. It should be so marked, however, whenever it is passed outside the department to ensure that it is afforded appropriate protection.*

GUIDELINES FOR TOP SECRET, SECRET,CONFIDENTIAL AND RESTRICTED

These four classifications cover information that requires protection for national security reasons. Most national security information would be adequately protected by the classifications CONFIDENTIAL or RESTRICTED. The classification SECRET should be used sparingly. Very little national security information warrants the classification TOP SECRET, which should be used with the utmost restraint.

TOP SECRET	Compromise of information would damage national interests in an exceptionally grave manner

- threaten directly the internal stability of New Zealand or friendly countries
- lead directly to widespread loss of life
- cause exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of extremely valuable security or intelligence operations
- cause exceptionally grave damage to relations with other governments
- cause severe long term damage to significant national infrastructure

SECRET	Compromise of information would damage national interests in a serious manner

- raise international tension
- damage seriously relations with friendly governments
- cause serious damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of valuable security or intelligence operations
- seriously damage the internal stability of New Zealand or friendly countries
- shut down or substantially disrupt significant national infrastructure

CONFIDENTIAL	Compromise of information would damage national interests in a significant manner

- materially damage diplomatic relations (i.e. cause formal protest or other sanction)
- cause damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations
- damage the internal stability of New Zealand or friendly countries
- disrupt significant national infrastructure

RESTRICTED	Compromise of information would be likely to affect the national interest in an adverse manner

- affect diplomatic relations adversely
- hinder the operational effectiveness or security of New Zealand or friendly forces
- affect the internal stability or economic well-being of New Zealand or friendly countries adversely

GUIDELINES for HANDLING RESTRICTED, SENSITIVE or IN CONFIDENCE INFORMATION

INTRODUCTION

Chief Executives are responsible for determining the levels of protection for RESTRICTED, SENSITIVE or IN CONFIDENCE[1] information to be applied within their departments. A Risk Management[2] approach is to be taken to achieve the protection as cost effectively as possible. The following publications are to be used as guidelines:

- The New Zealand Security of Information Technology (SIT) series of Publications issued by the Government Communications Security Bureau (GCSB).
- AS/NZ Standard 4444: *Information Security Management* and AS/NZ Standard: *Information Security Risk Management* (yet to be issued).

The levels of protection are to ensure that:

- Information should be held, processed, transmitted and destroyed with discretion to avoid opportunistic access by unauthorised people and make accidental compromise highly unlikely.
- All obligations to protect information provided by third parties are met.
- The release of RESTRICTED, SENSITIVE or IN CONFIDENCE information outside Government places it at no greater risk than if the Department concerned continued to hold it.
- Departmental staff are told about the level of protection required. Those outside Government should also be given similar guidance.

[1] This Appendix provides guidelines for protecting RESTRICTED, SENSITIVE and IN CONFIDENCE information. The rules for protecting TOP SECRET, SECRET and CONFIDENTIAL information are unchanged and contained in the manual *Security in Government Departments*.

[2] Risk management as defined in the Australia/New Zealand Standard 4360 – Risk Management

HANDLING AND/OR TRANSMISSION OF 'RESTRICTED' OR 'SENSITIVE' INFORMATION

Principles and clearance level	▪ Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. ▪ Only staff cleared by the department to access RESTRICTED or SENSITIVE level or above are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.

ELECTRONIC TRANSMISSION	▪ All RESTRICTED or 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	▪ 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: - 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 - Encryption
ELECTRONIC DISPOSAL	▪ Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
PAPER TRANSMISSION	▪ May be carried by ordinary postal services including commercial courier firms, provided the envelope/package is sealed and the word RESTRICTED or SENSITIVE is not visible. ▪ The outer envelope should be addressed to an individual by name and title. RESTRICTED or SENSITIVE mail for/from overseas should be carried by diplomatic airfreight. ▪ 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.
PAPER STORAGE	▪ Follow storage guidelines in *Data Management Standard for NZ Government* or Archives NZ Storage Standard NAS 9901 *Storage of Public Records or Archives* or in-house Records Management policy.
PAPER DISPOSAL	▪ Disposed of or destroyed in a way that makes reconstruction highly unlikely.

HANDLING AND/OR TRANSMISSION OF 'IN CONFIDENCE' INFORMATION

Principles and clearance level	▪ Information for official use, with consideration of 'need to know' principle

ELECTRONIC TRANSMISSION	▪ An appropriate statement should accompany all IN CONFIDENCE information transmitted via e-mail or Fax. ▪ It should outline legal responsibilities and notification/destruction instructions if the incorrect party receives it. ▪ IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text. ▪ Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in government agencies). ▪ All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.
ELECTRONIC STORAGE	▪ Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: - 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	▪ Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
PAPER TRANSMISSION	▪ May be carried by ordinary postal services or commercial courier firms as well as mail delivery staff in a single sealed envelope. ▪ The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.
PAPER STORAGE	▪ IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments. ▪ It should be noted that IN CONFIDENCE material may not always be labelled as such, particularly where it is never passed outside the responsible department.
PAPER DISPOSAL	▪ Disposed of by departmental arrangement that make compromise highly unlikely.