Review of DPMC Systems and Practices in relation to the Security of Sensitive Information

David Henry

23 June 2006

TABLE OF CONTENTS

PO Box 48 044
Silverstream
UPPER HUTT

23 June 2006

Maarten Wevers
Chief Executive
Department of the Prime Minister and Cabinet
WELLINGTON

Review of Department of the Prime Minister and Cabinet (DPMC) Systems and Practices in relation to the Security of Sensitive Information

1. Executive Summary

Introduction

1.1 DPMC operates at the very heart of executive government by providing impartial advice and support to the Prime Minister, the Governor- General and the Cabinet. The nature of government business requires classified information to be protected against unauthorised disclosure.

This review

1.2 This report reviews DPMC security systems, with particular reference to how DPMC manages classified information in the public policy and personal privacy areas. The term "cabinet papers" includes Cabinet Committee papers, agenda and minutes. The term "classified" means information to which one of the current 6 classifications (4 for national security information and 2 for public policy/personal privacy information) is required to be applied.

1.3 The review also required me to look more broadly at the handling of classified information in Ministers' offices and government agencies, the adequacy of the classification system and the procedures for releasing Cabinet papers.

Managing Security Risks- preliminary comment

1.4 Managing security risks is no different from managing other business risks. Risks cannot be eliminated but they can be managed by systematically identifying their causes, likelihoods, consequences and the remedial action needed. One common concept in security risk management is that of "defence in depth", that is, the setting up of multiple barriers to protect information rather than relying on one. At the same time the barriers must not be so high that they stop people doing their job.

The Security in the Government Sector Manual (2002)

1.5 This is the “bible” on security that government organisations are required to use. DPMC is chair of the Interdepartmental Committee on Security (ICS) which is the author of the Manual. The ICS should be reconvened to update the manual in the light of experience over the last 5 years.

DPMC Security Policy

1.6 DPMC has good systems and practices that generally follow the government-wide guidelines set out in the *Security in the Government Sector* Manual. Specifically the Cabinet Office sets and follows high standards including a clear desk policy and “defence in depth” against unauthorised disclosure of official information .

1.7 Some improvements are needed within DPMC. DPMC should issue its 2004 draft Security Policy and present it to staff. Branch Security Plans need to be documented and reviewed. Ongoing awareness training for all staff is required. Regular checks of compliance should be carried out by management. The clear desk policy for classified material should be part of those checks.

DPMC Recruitment and Selection of Staff

1.8 DPMC follows good practice in recruitment and selection of staff. It could do more pre-employment checks itself, specifically criminal record checks and, depending on position, credit checks. DPMC should also review the vettings it requests from the New Zealand Security Intelligence Service (SIS) to ensure that they are commensurate with the level of access to information that the employee will have.

DPMC Induction of Staff

1.9 Induction by the department follows good practice. Some improvements are needed, mainly the introduction of ongoing security awareness training.

Disposal of Classified Material

1.10 The disposal of classified material now follows good practice. Changes made by the Policy Advisory Group following a security breach are appropriate.

Handling Classified Material in Ministerial offices and departments

1.11 There appears to be over- reliance in Ministers’ offices on physical access security to protect classified information. The current policy agreed by Cabinet in 2001 and promulgated in Cabinet Office Circular CO (01) 10 is that all Cabinet documents should be locked away securely when not in use. This policy should be reissued to Ministers and their staff and to government organisations.

The Current Classification System for Cabinet papers of a Public Policy or Personal Privacy nature

1.12 A third classification "Highly Sensitive" should be added to the two classifications currently used and detailed guidelines and rules designed for it.

Public release of cabinet papers

1.13 The current system of decision making on release is appropriate. The standard format for cabinet papers set out in the *Step by Step Guide* could be extended to require a recommendation, on a case by case basis, regarding proactive release. The Cabinet Office should consider becoming the publisher of record for all released cabinet papers through its website.

Detailed recommendations

1.14 Recommendations appear throughout the body of the report and are listed at paragraph 23.

2. Introduction

2.1 In May 2006 an employee of DPMC breached security in relation to commercially sensitive information. The breach was subsequently investigated by the State Services Commissioner (SSC). The SSC's report dated 16 May 2006 can be found at: www.ssc.govt.nz.

2.2 In your public response to that report you stated that "further work would be undertaken to assess existing procedures and ensure risks are mitigated". Hence this review.

3. This Review

3.1 On 19 May 2006 you appointed me to review all of the systems in DPMC that are designed to ensure that sensitive information is handled with the required confidentiality and discretion. In addition the review was to examine three other issues: first, whether classified Cabinet papers are handled appropriately in Ministers' offices, government departments and agencies; secondly, whether the current security classification system for cabinet papers of a highly sensitive public policy nature is adequate; thirdly, whether additional policies are required on the public release of cabinet papers.

4. Terms of Reference

4.1 The detailed Terms of Reference are at Appendix 1.

5. DPMC-Its Role and Functions

5.1 DPMC is a department of the Public Service. It operates at the heart of executive government. It has 121 staff. Its role is to provide impartial advice and support to the Prime Minister, the Governor-General and the Cabinet. It is organised into 6 business units. Those units are

- Cabinet Office
- Government House
- Policy Advisory Group
- Corporate Services Unit
- Domestic and External Security Group
- External Assessments Bureau.

5.2 All business units have some access to classified information. The External Assessment Bureau and the Domestic and External Security Group have access regularly to national security information at the highest levels. The other groups have access regularly to classified information of a public policy or private nature but not to highly classified information of a national security nature.

6. Protecting and Classifying Official Information

6.1 The current system for protecting official information from unauthorised disclosure was introduced in 2001. The application of the new system to cabinet papers took effect from 1 August 2001 and was promulgated by Cabinet Office Circular CO (01) 10 (reproduced at Appendix 3). The system is comprehensively set out in the *Security in the Government Sector* Manual (published at www.security.govt.nz). The classification system is also described in the *Cabinet Manual* (published at www.dpmc.govt.nz) and the *Step by Step Guide* (also at www.dpmc.govt.nz).

6.2 The system is based on classifying information using principles and guidelines which enable a determination to be made of the degree of harm that could result from unauthorised disclosure. Standard rules (for example regarding storage) are then applied to determine how the information so classified is to be protected.

6.3 Information is first divided into two prime categories -

National Security information, being information whose unauthorised disclosure could threaten the security or defence of New Zealand or affect New Zealand's international relations.

Policy or Personal Privacy information, which is not National Security information, whose unauthorised disclosure could prejudice law and order, impede the effective conduct of government business, or damage or prejudice New Zealand's economic interests.

6.4 ***National Security*** information has four classifications which are, in ascending order of importance:

- Restricted
- Confidential
- Secret
- Top Secret.

6.5 These national security classifications are mainly applicable to material handled by the Ministry of Foreign Affairs and Trade, Defence, the External Assessment Bureau, the Domestic and External Security Group and the intelligence agencies.

6.6 ***Policy and Personal Privacy*** information has 2 classifications which are, in ascending order of importance:

- In Confidence
- Sensitive.

6.7 The vast majority of Cabinet papers fall into the *Policy and Personal Privacy category.*

6.8 Endorsement markings may be added to a paper, for example to indicate the nature of the information it contains. Common endorsements include " Budget" and "Commercial". Thus the Cabinet paper which was the subject of the May 2006 security breach was marked "Commercial: Sensitive".

7. Relationship with the Official Information Act 1982

7.1 The classification system was designed to be consistent with the Official Information Act 1982.

7.2 The purposes of that Act are:

- to increase progressively the availability of official information to the people of New Zealand
- to provide for proper access by each person to official information relating to that person
- to protect official information to the extent consistent with the public interest and the preservation of personal privacy.

7.3 The Official Information Act lists both conclusive and non-conclusive reasons why information may be withheld. The classification allocated to a document is not in itself decisive and each case must be considered in terms of the Official Information Act.

8. Communication of the 2001 Classification System

8.1 The 2001 Cabinet Office circular (Appendix 3) advised Ministers, Chief Executives, parliamentary officers and senior private secretaries in Ministers' offices that the revised classification system would apply to Cabinet papers from 1 August 2001 and required them to ensure that all staff were familiar with the new procedures. Crown entities and other government agencies handling cabinet papers were also to be informed. The circular included an instruction that "…all cabinet documents should be kept in secure lockable storage when not in use".

8.2 In April 2001 departmental security officers were given presentations on the new procedures by DPMC and the SSC. The purpose was to assist those officers to train staff in their organisations on the new procedures. Compliance audits were to take place in 2002 but did not eventuate.

8.3 It was also decided to rewrite the basic security instructions contained in the manual and put that new manual on- line. This was done in 2002 and renamed "*Security in the Government Sector*".

8.4 There was thus some across the board activity on security issues in the government sector in 2001 and 2002.

9. The Security in the Government Sector (SIGS) Manual 2002

9.1 The purpose of the manual is to provide a consistent framework within which government organisations develop their own security policies.

9.2 The Manual is mandatory for government departments, ministerial offices, the NZ Police, the NZ Defence Force, the SIS and the Government Communications Security Bureau (GCSB). It is also made available to State Owned Enterprises and Crown Entities.

9.3 The drafting of the manual and its regular updating is the responsibility of the Interdepartmental Committee on Security. The committee is responsible for formulating and co-ordinating the application of all aspects of security policy across government and setting common minimum standards. The committee is chaired and serviced by DPMC and includes representatives of the Ministry of Defence, the Defence Force, the Ministry of Foreign Affairs and Trade, the SSC, the Police, Cabinet Office, the SIS and the GCSB.

10. Key Principles of the SIGS Manual

10.1 Chief Executives are responsible for implementing and managing effective security arrangements within their organisations based on risk assessment.

10.2 Security should be integrated into an organisation's philosophy, practices and plans and not seen as something separate.

10.3 Each organisation's security policy should provide:

- general guidance on security roles and responsibilities
- clear definitions of responsibility for the protection of classified material
- more detailed guidance for specific sites, systems or services
- an ongoing programme of user awareness and education.

10.4 Protective security relies on "defence in depth" which means combining several measures to make unauthorised disclosure difficult, including

- the "need to know "principle which limits access to those who need the information to carry out their duties
- a classification system for information that needs protection
- personnel security
- physical security
- controls built into departmental IT systems.

10.5 Detailed security instructions should be used to implement the policy. (The manual suggests topic headings for such instructions including the control, transmission, storage and destruction of classified documents.)

10.6 There needs to be periodic reviews of the security policy's effectiveness and the level of user compliance.

10.7 Each organisation should have a Departmental Security Officer with direct access to the Chief Executive whose responsibilities include ongoing security awareness and training.

11. Security Policies in relation to Employees

11.1 The SIGS Manual identifies that a key part of security policy is to manage the risk posed by employees. The vast majority of employees are of course trustworthy but security policy needs to manage the risks posed by the few who are not.

11.2 The checking of prospective government employees prior to appointment normally takes place when an applicant is the top, or one of the top, candidates and is carried out with the applicant's permission. Checks by the employer commonly include

- verification of identity
- completeness and accuracy of the curriculum vitae including academic qualifications
- structured discussions with referees
- a criminal record check with the Ministry of Justice.

11.3 The granting of a *security clearance* is always a decision for the employer. Before granting a clearance SIS vetting is mandatory for an employee who has regular access to national security information at "Confidential" level or above. It is however often sought for other employees. SIS acceptance of a vetting request is based on the assumption that the employer has carried out the checks listed in paragraph 11.2. The depth of the SIS vetting depends on the level requested by the employer which in turn may determine how long the vetting takes. Currently, vetting at Secret and Top Secret levels can take 6 months.

12. Security Policies in relation to Contractors and other third parties

12.1 The SIGS Manual identifies the risks posed by contractors and other third parties who may have access to premises including people who have access after hours, such as cleaners. It is good practice to require the contracting employer to:

- have regard to the department's Security Policy
- carry out employment checks including a criminal record check through the Ministry of Justice
- agree to confidentiality requirements in the contract
- provide an up to date list of cleared employees on a regular basis.

13. Risk Management Frameworks Generally

13.1 The SIGS Manual requires chief executives to employ a risk management approach in developing security policy and instructions. There are many different frameworks but they all use some form of systematic analysis to identify the risks (that is exposures to specific events) which the organisation faces, to assess the *likelihood* of the risks occurring and the *consequence* if those risks do occur. Actions to mitigate *likelihood* and *consequence* are then identified.

13.2 Assessing security risks is therefore a subset of the organisation's wider risk management activity.

13.3 Responsibility for managing specific risks may be placed on individual managers or groups of managers. It is common for the senior management team to regularly review an updated risk management inventory. It is also common for the organisation's Internal Audit Programme to be designed to audit identified risks over time.

13.4 A problem experienced by most organisations is in inculcating risk management thinking throughout the organisation.

14. The DPMC Risk Management Framework

14.1 DPMC has been improving its risk management framework. In May 2005, stage one of the project was completed, being the identification and assessment of the key risks in achieving the department's outcomes (effectively a strategic risk assessment).

14.2 One of the top 20 risks identified in May 2005 was "Confidentiality" defined as "Risk of actual or perceived release of confidential information either deliberately or inadvertently". The risk was assessed as low likelihood and high consequence. Controls on managing the risk were judged to be "strong".

14.3 The second stage of the project is to assess current risk management practices and implement a living risk management framework in the organisation. That will assist the further development of DPMC's security policy.

15. The DPMC Security Policy

15.1 In line with the SIGS Manual, DPMC drafted a departmental security policy which was close to promulgation by May 2004. Because of work pressures the policy was not promulgated. However, DPMC management believe much of the policy is operating in practice.

15.2 The draft DPMC Security Policy applied the principles of the SIGS Manual to the DPMC environment. Some features of the DPMC Security Policy were:

- A Departmental Security Officer was designated to have overall responsibility for security policy.
- The relative security risks faced by each business unit of DPMC differ and thus each unit was to customise the policy in relation to those risks.
- Each unit was to appoint a Branch Security Officer to actively manage security including monitoring staff awareness and compliance.
- There was to be a "clear desk, clear computer screen" policy to protect classified information. Hard copy classified information was to be locked away when not being used.
- Classified material was to be disposed of according to its level. *In Confidence*, *Sensitive* and *Restricted* waste was to be placed in special Security Bins for later destruction. *Secret* and *Top Secret* was to be destroyed under the supervision of the Branch Security Officer by shredding.
- New staff were to be given a copy of the DPMC Security Policy along with other standard documents such as the Code of Conduct.
- Most DPMC staff were to be vetted by the SIS to "Confidential Level" with some staff vetted at higher levels.
- DPMC Security Policy was to be regularly reviewed and updated.

16. Internal Audit of DPMC Security,

16.1 DPMC's Internal Audit Committee included a security audit in its 2003/2004 programme. The audit was completed in April 2004. The auditor had the draft DPMC Security Policy available to him.

16.2 The auditor's overall conclusion was

".. the general level of protective security in DPMC currently meets departmental security policy standards together with the requirements of the Security in the Government Sector Manual and is appropriate to the risks faced."

16.3 The audit noted however that there was no formalised security- related training or awareness raising in the business units. The auditor saw the launch of the DPMC Security Policy as the first step in tackling this.

17. Part 1 of the Terms of Reference: DPMC Recruitment, Selection, Induction and Training

17.1 Part 1 of the Terms of Reference direct me to

"*Review and identify any areas for improvement in the manner in which DPMC handles its recruitment, selection, induction and staff awareness training procedures".*

17.2 I have examined DPMC's documented policies, the relevant government-wide policies and the practices of a number of government departments. I have also reviewed a sample of DPMC appointment files to see whether DPMC policies were operating in practice.

Recruitment and Selection

17.3 DPMC follows a robust process in relation to recruitment and selection. Those policies include open advertising, detailed job descriptions, careful short listing, structured panel interviews, identity and qualification checks and comprehensive write ups. DPMC does not however carry out criminal record checks in all cases as I note in paragraph 18.3 under the second part of the terms of reference. Apart from criminal record checking there are only minor improvements that might be made to recruitment practices and I will include them in the recommendations.

17.4 DPMC also routinely arranges psychometric testing of employees by a specialist firm. The depth of that testing depends on the nature of the position and is not expensive in most cases.

17.5 I noted that DPMC, in common with other government departments, does not routinely carry out credit checks which might disclose a prospective employee has poor financial management. I suggest at paragraph 18.10 that a credit check is useful in some cases.

17.6 There is emphasis throughout the process of recruitment and selection on the applicant's honesty and the need for confidentiality but there is no standard comprehensive statement which encapsulates the general responsibilities to maintain security policy and the specific responsibility to protect official information as suggested by the SIGS Manual. A comprehensive but simple statement could be usefully added to position descriptions which would then ensure that interviews with referees and psychometric testing give appropriate weight to security issues.

Induction and Staff Awareness Training Procedures

17.7 DPMC sends a comprehensive letter of offer to the chosen applicant. (The offer of employment is conditional on the employee obtaining a security clearance following SIS vetting. This is discussed further in paragraph 18.4). The letter of offer also attaches, amongst other things, a declaration of confidentiality for the appointee to complete as well as the security questionnaire required by the SIS.

17.8 DPMC, in common with other government departments, uses comprehensive induction checklists to introduce a new employee to the department. The first checklist covers steps to be taken prior to commencement and the second covers the employee's arrival on the job.

17.9 The checklists detail administrative steps such as obtaining information for payroll and tax purposes. But the checklists also include more substantive issues such as providing the Code of Conduct and obtaining sign off of declarations on confidentiality. What is not documented by the checklist is how and to what degree the employee has been taken at induction through the important policies contained in documents such as the Code of Conduct, the Information Systems Code of Practice and the DPMC Security Policy.

17.10 I do not see any ongoing formalised programme of staff awareness training on such issues as security policy, code of conduct or ethics. Given the number of things competing for the employee's attention on arrival and the complexity of the issues that may be faced later, formalised training is highly desirable.

17.11 There are a number of good models in the public sector which might be usefully studied in designing initial and ongoing training. I was advised of two agencies that use on-line training in security awareness aimed at new staff and refreshing the knowledge of experienced staff. Another department is also going down that path. New staff complete the on-line training at their own pace over the first few weeks of employment. Completion is monitored by management. The two organisations using this approach are Land Information New Zealand and the Accident Compensation Corporation. (I have given copies of these training packages to the DPMC Human resources Manager.)

17.12 There is also the 2003 State Services Commission package "Walking the Line" which deals with ethical issues faced by public servants. It is published at www.ssc.govt.nz .The package is based on group discussion of relevant case studies of ethical dilemmas. It has been used to some extent in the past within DPMC. It requires adaptation to the needs of each organisation. For example the dilemmas posed by access to commercially sensitive information would be relevant to DPMC.

17.13 To implement these (and other recommendations in this report) will require additional resources to be allocated to DPMC's Corporate Services Unit.

Recommendations

Security Policy

1.1 Issue the DPMC Security Policy and hold staff briefings on it.
1.2 Prepare a simple guide on the main points for staff to hold.
1.3 Implement the Security Policy and institute compliance checks.
1.4 Reconvene the Interdepartmental Committee on Security to update the "Security in the Government Sector" Manual.

Position (Job) Descriptions

1.5 Standardise the format of position descriptions.
1.6 Ensure that the position description lists the job competencies required.
1.7 Determine the relative importance of each competency by weighting them and use those weightings to assist short listing decisions.
1.8 Include in the position descriptions explanations of the general and any specific responsibilities under the security policy.
1.9 Include in the position descriptions the requirement to be vetted through criminal record checks and, where appropriate, SIS checks.

Selection

1.10 Standardise the format of the write up of appointments.
1.11Explicitly use the competencies and their weightings in the write up.
1.12 Review the templates used for referee interviews to add to the normal level of questions on honesty deeper questions on the prospective employee's discretion and ethics.

Induction

1.13 Include the proposed simple guide to security policy (see recommendation 1.2) in the induction package.

1.14 Redesign the induction checklists to separate out the purely administrative tasks and to document that the substantive tasks have been completed.

Staff Awareness Training

1.15 Design a programme of initial and on going training covering security and related issues and in doing so review the applicability of self-paced on-line training as developed by some government agencies.
1.16 Require Branch Security Officers to keep up to date through training and to schedule regular updates for staff on security issues.
1.17 Consider further ethics training by customising to DPMC needs the State Services Commission's 2003 "Walk the Line" Package.

Corporate Service Resources

1.18 Review the adequacy of the current resources available to the Corporate Services Unit to implement the recommendations in this report.

18. Part 2 of the Terms of Reference: DPMC's Internal Security Clearance Policies, and Staff Training and Awareness on Information Confidentiality and Conflicts Of Interest

18.1 Part 2 of the Terms of Reference requires me to

" Review and identify any areas for improvement with regard to DPMC's internal security clearance policies and procedures, and staff induction/training and awareness on confidentiality of information and conflict of interest issues".

DPMC's Internal Security Clearance Policies

18.2 Standard security clearance policies in line with the SIGS Manual are described in paragraph 11.

18.3 DPMC clearance policies are generally in line with those policies with one exception. The exception is that DPMC procedures have not routinely included a criminal record check, perhaps on the basis that this will be done during SIS vetting. The employee is asked at the interview to disclose anything that would prevent a clearance being issued.

18.4 DPMC has a written policy on the level of SIS vetting required for each employee. The level is determined primarily by the highest classification of official information that the employee regularly deals with. The policy provides that many staff must be vetted to Secret or Top Secret level but states that staff being vetted at Secret Level or below can be employed on condition that their employment may be terminated if a security clearance cannot be given. The fact that the employee does not have a clearance in the meantime may require special measures to control the employee's access to information or premises. That is difficult to achieve in a busy department.

18.5 Currently, SIS vetting may be subject to substantial delays. For example at 22 May 2006 there were 9 people employed in DPMC waiting for the completion of SIS vetting including some who have been employed for more than 6 months. The use of termination of employment clauses was predicated, one assumes, on the basis of timely security clearances.

18.6 The delays in SIS vetting are caused by 3 factors. First, the employee may be slow in completing the necessary vetting questionnaire. DPMC could reduce this delay by requiring the employee to have the form completed on arrival and more actively managing the situation if the employee has not done so.

18.7 The second cause of delay is the level of SIS vetting requested by DPMC. This policy requires review to see whether some requests could be downgraded to the less time consuming "Confidential" rating or even eliminated. If DPMC implements its Security Policy a review should enable some downgrading or elimination to occur.

18.8 The third cause of delay is the time taken by the SIS. In April 2006 the Director of the SIS advised departments that the security vetting service was under significant pressure resulting in an excessive waiting time. He noted that the Service was working on a permanent solution but in the meantime he asked departments to review the need for vetting and ensure it was commensurate with the level of access the person requires. As noted in the previous paragraph DPMC needs to do this.

18.9 DPMC needs to manage risk by increasing its own checks as employer. The first change required is to routinely request a criminal record check though the Ministry of Justice. The Ministry handles approximately 150 000 checks a year emanating from a wide range of organisations. Requests from government departments were almost 2000 a month as at June

2005. The Official Information Act and the Privacy Act require the information to be released within 20 working days. The Ministry currently takes about 10 days to provide the information.

18.10 The second change suggested would be to institute credit checks on a case by case basis with the permission of the prospective employee. Credit checks can be done quickly and easily. A credit check may raise underlying issues such as trustworthiness and poor personal management. Whilst a poor credit record or a history of defaults may not be conclusive in the decision to employ or not, such issues may need to be explored with the prospective employee before the decision is taken.

Staff Training and Awareness on Confidentiality of Information and Conflict of Interest Issues

18.11 The DPMC Code of Conduct given to appointees at induction is very clear about the need for confidentiality and refers to the declaration of confidentiality that staff are required to sign. It also refers to the special rules surrounding the handling of classified information. What is lacking is a comprehensive approach to staff awareness and training based on the DPMC Security Policy. Recommendation 1.15 already cover these issues.

18.12 The DPMC Code of Conduct has succinct advice for staff in respect of real or perceived conflicts of interest. For example it specifically requires an employee to declare to "a senior member of staff" financial interests in circumstances where it could be perceived that the employee stands to benefit from information gained through his or her job. I understand that DPMC management has in the past reminded staff of the need to declare conflicts of interest when specific policy issues were under government consideration. I note also that the Cabinet Office "Conduct Guidelines" have specific advice, including the need to inform the Secretary of the Cabinet in certain situations.

18.13 It would be useful to clarify in the DPMC Code of Conduct the procedural rules for raising or declaring conflict of interest issues. These could include specific advice on who to raise the issue with and comment on possible "work arounds" such as a temporary transfer to other duties.

18.14 Apart from the initial briefing at induction there is no formalised staff training on conflict of interest issues. I have discussed this earlier under Part 1 of the Terms of Reference and Recommendation 1.17 deals with the issue of formalised ethics training tailored to the department's work.

Recommendations

Pre- Employment Checks

2.1 Extend DPMC pre-employment checks to routinely include criminal record checks through the Ministry of Justice, having obtained the permission of the proposed appointee.

2.2 Extend DPMC pre-employment checks to include financial credit checks, on a case by case basis, with the permission of the proposed appointee.

Vetting Requests to the SIS

2.3 Review the levels of security vetting being requested from the SIS to reduce the number of requests and to ensure the vettings requested are commensurate with the level of regular access the employee will have in the future to national security information classified "Confidential" or higher.

2.4 Require employees who are to be vetted by the SIS to bring the completed security questionnaire with them on their first day and actively manage any failure to do so.

2.5 Ensure managers responsible for an employee awaiting SIS vetting are aware of that status so that they may manage access appropriately.

Conflicts of Interest

2.6 Clarify and promulgate the procedural rules surrounding the raising or declaration of conflicts of interest and update the DPMC Code of Conduct.

19. Part 3 of the Terms of Reference- DPMC's Policies on the Secure Disposal of Classified Material

19.1 Part 3 of the Terms of Reference require me to

"Review and assess DPMC's policies and practices in relation to the secure disposal of classified material".

19.2 The SIGS manual gives both general and specific guidance on the disposal of classified material. Classified material is to be held in an appropriate container separate from other waste. Destruction should take place as close as possible to the point of origin. Destruction is to be under the strict supervision of a staff member with the appropriate security clearance. The supervising staff member is to accompany the material to the point of destruction and ensure that destruction is complete.

19.3 The methods and completeness of destruction vary according to the level of classification. For example " In Confidence " material is to be "disposed of with care to make compromise highly unlikely" whereas the more highly classified material graded " Sensitive" or above is to be disposed of in a way which makes "reconstitution highly unlikely", for example by adequate shredding. Minimum standards for shredders took effect from 1 July 2004. Only cross-cut shredders are to be used and their level of performance is to increase in line with the classification of document to be destroyed.

19.4 DPMC's disposal policy is summarised in its draft May 2004 Security Policy. The policy refers readers to the SIGS Manual and says that the security disposal bins may be used for "In Confidence", "Sensitive" "Restricted" and "Confidential" material. More highly classified material is to be shredded within DPMC.

19.5 DPMC has contracted with a specialist firm to provide a secure destruction service to Floor 10 of the Beehive (the Cabinet Office) and Floor 8 (the Policy and Advisory Group). The contractor provides the security disposal bins and shreds their contents in a sealed shredding vehicle brought to the parliamentary complex. The security bins are locked. (The destruction of classified waste in other parts of the parliamentary complex is subject to separate contracts entered into by Ministerial Services and Parliamentary Service which require review by those agencies.)

19.6 Staff of the Cabinet Office themselves place material directly into the bins which are kept in a secured room. The secured room is on Floor 10 of the Beehive. That floor is not accessible to the public.

19.7 In contrast staff of the Policy Advisory Group have had the practice of placing material in special trays or baskets to be cleared by a designated DPMC messenger at the end of the day. The messenger then placed the material collected into the security disposal bin kept in the Head Messenger's office.

19.8 Full bins are kept in a secure facility under the control of the Head Messenger. When a number of bins are full the contractor is notified by the Head Messenger and the bins are transported by the Head Messenger and his team directly to the sealed shredding vehicle. The contents are then destroyed under supervision.

19.9 The procedures described are generally in accordance with the principles of the SIGS Manual and the draft DPMC Security Policy. Destruction inside the parliamentary complex, rather than transferring the material elsewhere, is a strong feature.

19.10 The exception has been the practice in the Policy Advisory Group of using intermediate trays or bins to hold classified material for later transfer to the security disposal bins. I am

pleased to see that the Policy and Advisory Group has now changed its practice and deposits classified waste directly into the locked security disposal bins.

19.11 I have examined the contract between DPMC and the firm providing the secure destruction service and I think there are some issues which need review. I do not see these as serious given the controls operating in practice. First, there is no provision in the contract which requires the contractor to warrant that their employees, or any subcontractors, handling the bins have been subject to a security check, such as a criminal record check through the Ministry of Justice. Secondly, there is no provision that requires details of authorised employees to be provided to the DPMC Security Officer before employees commence duties. Finally, there is no specification of the standard of shredding to be achieved.

19.12 In addition to using the contractor's sealed shredding vehicle some waste may be shredded directly by DPMC officers. As noted earlier the specifications for shredders were upgraded with effect from July 2004. DPMC needs to ensure that its shredders meet the required standards which are set out in Part 2 of the Protective Security Manual issued to Departmental Security Officers.

Recommendations

Disposal of Classified Waste

3.1 Review DPMC's contract with the contractor supplying the secure destruction service to include warranties regarding its employees and to specify the standard of shredding to be achieved.

3.2 Review current shredders against the specifications set out in the Protective Security Manual and schedule replacement as necessary.

3.3 Carry out spot checks in line with the DPMC Security Policy to monitor compliance with the disposal policies for classified waste.

3.4 Forward a copy of this report to Ministerial Services and Parliamentary Service to take into account in any review of the other destruction services provided to the parliamentary complex.

20. Part 4 of the Terms of Reference: The Handling, Access and Storage of Classified Cabinet Papers in Ministers' offices, departments and other agencies.

20.1 Part 4 of the terms of reference require me to

" Review and assess whether classified cabinet papers are being handled, accessed and stored in Ministers' offices, departments and other agencies handling cabinet material, in accordance with current guidelines; and identify if any improvements to current policies, procedures, and guidance are required".

20.2 This part of the review follows a Cabinet directive of 8 May 2006.My approach has been to examine how such matters are handled inside the DPMC and then extend the review by sampling outside the DPMC. A list of people and organisations consulted is at Appendix 4.

20.3 The current guidelines for handling accessing and storing classified Cabinet papers are in the 2001 Cabinet Circular (reproduced at Appendix 3) and the SIGS manual.

The Flow of Cabinet papers

20.4 Cabinet papers are received from the Minister's offices. The papers are accompanied by two forms.

20.5 The first form is the Cab *100* which is a certificate by the relevant department and by the Minister on the consultation process that has been followed in formulating the proposals.

20.6 The second form is the *Cab 101* cover sheet which is in two parts. The first part is for the Minister's office to indicate whether the paper is for Cabinet or for one of the 8 or so Cabinet Committees and the security classification allocated to the paper. The second part of the *Cab 101* enables the Cabinet Office to record its actions on the paper including preparation of the "top" summary, allocating reference numbers and determining how the paper is to be handled during distribution.

20.7 The Cabinet Office may also review the classification allocated by the Minister's office and if necessary adjust it in consultation with the Minister's Office.

20.8 There is no documentation or sign off by the person in the Minister's office (or department) who has made the classification decision. (It would also be desirable for a provisional classification to be allocated when the policy paper is being worked up- some departmental document management systems require this already).

The Distribution of Cabinet papers

20.9 The Cabinet Office Registrar supervises the copying of Cabinet papers for distribution to Minster's offices in accordance with a detailed process which enables Ministerial staff to prepare the Minister's file for the meeting. This is a complex and time- critical job with more than 2000 papers being handled a year.

20.10 Under the control of the Registrar the DPMC messengers prepare batches of papers for each Minister and deliver them by hand around the Beehive. The papers are carried in a concertina folder and are handed over in bulk. The hand over is evidenced by an authorised person in the Minister's office who checks the batch of papers for completeness before signing. If there is no authorised person available the batch is brought back to the Registry.

20.11 The batch of papers handed over to the authorised person in the Minister's office may include a paper in a separate envelope if its classification so warrants. In such a case the messenger making up the batch will have received the paper in a sealed envelope from the Registrar with the reference number of the paper shown on the envelope.

20.12 In relation to most cabinet papers, being of a Public Policy or Personal Privacy nature, Cabinet Office instructions do not requires a separate envelope unless the paper has an additional endorsement "Personal to [Minister]" or otherwise indicates that it is for the Minister's eyes only. Thus a paper classified "Sensitive" would be handed over unenveloped if distributed inside the Beehive. This is in line with the SIGS Manual because the material is being moved by hand within the same building by officers who are authorised to handle such papers.

20.13 I have examined the enveloping issue in some depth and have concluded that changing the system is likely to increase the time for distribution to Minister's offices and is not warranted. Past experience has shown that over- use of separate envelopes will not only slow down the process but reduce the significance of the envelope to Ministerial staff and Ministers. (See however Recommendation 5.1 which suggests a third level of classification for public policy and privacy papers which would result in papers at that third level being separately enveloped.)

DPMC Policies and Practices

20.14 The Cabinet Office (including the Honours secretariat) has clear rules in respect of handling, accessing and storing cabinet papers. The Office operates a clear desk policy under which all working material is locked away at close of business or in the absence of the officer. The Office in the Beehive is not accessible by the public lifts. Rooms are also locked at night and key control is maintained. The registry of cabinet documents and other files is in a secure facility. Appointment papers going to Government House are enveloped and after signature returned to the originator.

20.15 The Policy Advisory Group has not operated to the same level of security in respect of classified documents as the Cabinet Office. It is accessible by lift although visitors must go through parliamentary security. The lack of screening between the offices and the core lift area makes security more difficult. I am pleased to see however that the Policy Advisory Group has recently moved substantially towards Cabinet Office standards, including adopting a clear desk policy. These changes needs to be actively monitored by group management.

20.16 The Corporate Services Group handles few classified cabinet papers but generally follows good practices.

20.17 The EAB and the DESG have exemplary multi- level security systems.

20.18 All parts of DPMC will however benefit from issue and implementation of the DPMC Security Policy (Recommendation 1.1)

Handling Access and Storage in Minister's Offices

20.19 There are, I am told, 29 Ministerial Offices. The Senior Private Secretary is the manager of the Minister's office and is responsible for organising the Minister's papers for Cabinet or the Cabinet Committee. The Senior Private Secretary is a public servant as are all ministerial staff. They are either employed by the Department of Internal Affairs (through that department's Ministerial Services branch) or are seconded from departments. There is steady turnover of staff, including turnover after each general election.

20.20 Ministerial Services have recently instituted criminal record checks through the Ministry of Justice. Previously, reliance was placed solely on SIS vetting. I commend the change of practice.

20.21 Knowledge of security and practices in respect of safeguarding information in Ministerial Offices vary. Senior Private Secretaries are not always able to enforce security rules.

20.22 There is as yet no comprehensive security policy for Ministerial staff to follow. In April 2006 the Departmental Security Officer for Ministerial Services issued new instructions on security and has generally been raising awareness with ministerial staff through monthly meetings. (As noted in relation to DPMC however there has tended to be a reliance on a briefing at induction but ongoing awareness training is needed.) There are a number of security officers involved in the Parliamentary complex- Ministerial Services, Parliamentary Service, the Clerk's Office and DPMC. A Parliamentary Complex Security Committee to better coordinate security policies across the complex is desirable and I have already recommended a copy of this report go to them.

20.23 In some Ministerial Offices the practice has been that a separately enveloped cabinet paper marked "Personal to " the Minister would be opened by the Senior Private Secretary in line with the wishes of the Minister. In others it would only be opened by the Minister, which is in line with the intent of the "personal to" endorsement. On 8 May 2006 Cabinet reminded Ministers and their staff of the correct procedure. I suggest in paragraphs 21.9 and 21.10 how a third security classification might reduce the use of the "Personal to" endorsement.

20.24 A clear desk policy is clearly not universal in Ministerial offices which means that people are relying mainly on physical security in the parliamentary complex. This is unwise. It does not fit with the "defence in depth "principle. I believe a change to a "clear desk" policy is needed in respect of classified information and that the support of Ministers is needed to make that a reality. A "Clear desk " policy means in a nutshell that classified material is secured when not being worked on and is locked away securely at the end of the business day. This is what Cabinet Office instructions already require (see Appendix 3).

Handling Access and Storage by government departments and other entities

20.25 Overall, handling access and storage is well controlled but the level of expertise and awareness varies according to the frequency which the department handles classified material. As expected, departments which handle national security information regularly- such as MFAT- have very well developed processes.

20.26 All departments had appointed departmental security officers and the majority had comprehensive security policies based on the SIGs manual although most policy documents need updating.

20.27 Expert assistance to government agencies is available from the intelligence agencies (SIS and GCSB), which are playing an active advisory role across government. Not all Departmental Security Officers attend briefing sessions.

20.28 There remains a difficulty however and that is the lack of a simple guide to action. It is daunting for the non-expert to be directed to the SIGS manual. I note that the Treasury has produced a simple laminated guide which says for each classification of cabinet paper how it is to be handled in both hard and soft copies including:

- what must be done
- what can be done
- what must not be done.

20.29 DPMC should review this laminated guide and issue a version of it to all government agencies.

On-going Security Awareness Training

20.30 Many agencies have difficulties in providing ongoing awareness training on security after the initial “burst” at induction. In paragraph 17.11 I comment on developments in on- line training which could assist.

Recommendations

Handling of Classified Cabinet Papers in Ministers’ Office and departments

4.1 The Cabinet Office should consider incorporating in the Cabinet paper process and in the "Step by Step Guide" a more formal documentation of the classification decision by Ministers’ offices or departments. The Guide should also discuss the application of provisional classifications at the policy formulation stage when the paper is being worked up.

4.2 DPMC should develop and issue to Ministerial offices and government agencies a simple guide to the handling, accessing and storage of classified cabinet papers along the lines of the model used by Treasury.

4.3 Cabinet should direct the Cabinet Office to repeat the 2001 instructions that a clear desk policy should be in place in Ministers’ offices and in government departments in respect of classified cabinet papers.

4.4 Government organisations should be encouraged to review developments in on-line security awareness training, including reviewing the training packages developed by LINZ and ACC.

21. Part 5 of the Terms of Reference: Improvements to the Current Classification System for Highly Sensitive Cabinet Papers of a Public Policy Nature

21.1 Part 5 of the Terms of Reference require me to

" Review and assess whether the application of the current security classification system is adequate for the protection of highly sensitive Cabinet material (of a public policy nature) and identify if any improvements to the system is required".

21.2 This is a response to a Cabinet directive dated 8 May 2006.

21.3 There are two classifications that can be applied to Cabinet papers of a Public Policy or Personal Privacy nature- *In Confidence* and *Sensitive.*

21.4 The two classifications have general descriptions which are then followed by specific guidelines. The general descriptions are -

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.

Sensitive – Compromise of information would be likely to damage the interests of the NZ government or endanger the safety of its citizens.

21.5 The two classifications are closely connected. Whilst each has its own guidelines the rating of "Sensitive" is also applied to information which meets the "In Confidence" guidelines where it is judged that the subject matter and degree of damage that would arise from unauthorised disclosure requires greater protection.

21.6 There are Cabinet papers of a public policy nature which are not easily managed under the current 2 classifications. For example all budget papers are automatically classified as "Sensitive" but a significant tax policy change might require more protection. The Cabinet Office has tended to work around this by marking some "Sensitive" papers as also " Personal to [the Minister]. But this means that no one other than the Minister is to see it. This may cause difficulties for the Minister. There is a good case for a third category of classification with its own additional protections.

21.7 If such a third category is to be added, namely *Highly Sensitive,* then the general description and specific guidelines would need to be drafted carefully to avoid overuse of this category. At the same time it would be appropriate to review the detail of the other 2 categories to ensure "fit" with the new category. Experience over the 5 years since the system was introduced could also be fed in.

21.8 A general description for "Highly Sensitive" could be

"Compromise of information would be likely to significantly damage the interests of the New Zealand government or widely endanger the safety of its citizens.

21.9 The issue is exactly what different rules would be applied if papers were classified as *Highly Sensitive* rather than *Sensitive.* One approach would be to treat the new classification as the equivalent of *Confidential* in the national security area and accessibility and handling would then follow the same rules. In practice this would impose significant compliance costs and it

would be better to have specific rules additional to the current rules for *Sensitive.* An additional rule should be that all *Highly Sensitive* papers must be enveloped in the Cabinet Office registry.

21.10 The third category would also have the advantage that an adviser in the Minister's office who has the appropriate level of clearance would be able with the Minister's permission to open the envelope and review the paper before providing advice.

21.11 The third category would not replace the endorsement currently available of "Personal to [the Minister]" but the need for this endorsement would be reduced. The current instruction, that no one other than the Minister is to open the envelope marked "Personal to", might then be consistently followed.

Recommendations

Improvements to the Current Classification System

5.1 That a third classification "Highly Sensitive" be introduced for cabinet papers of a public policy or personal privacy nature.

5.2 That the general description and detailed guidelines applicable to the "Highly Sensitive" category, and additional rules for handling, access and storage of them, be drafted with regard to the current principles applying to cabinet papers of a public policy or personal privacy nature.

5.3 That the general description and detailed guidelines of the current two categories " In Confidence" and " Sensitive" be reviewed in conjunction with the new category and in the light of experience since 2001.

5.4 That the "Personal to [Minister]" endorsement be retained and the current rule debarring access by persons other than the Minister be reinforced.

22. Part 6 of the Terms of Reference – Public Release of Cabinet Papers

22.1 Part 6 of the Terms of Reference require me to

" *Review and assess the procedures for providing Cabinet papers for public release, following a decision by Ministers to release the material, and consider whether additional policies or guidance should be provided".*

22.2 The current policy is summarised in the Cabinet Manual (paragraphs 6.25-6.28).

22.3 Most public releases result from a request under the Official Information Act. There is no blanket exemption under the Act for Cabinet papers and each request has to be considered in terms of the Act. The security classification of the paper is not decisive.

22.4 The decision to release is made by the Minister or department after any necessary consultation with other affected Ministers or departments. The Cabinet Office does not have to be consulted but is available for general guidance. Ministers and departments are required to keep a record of Cabinet papers released.

22.5 There is no central register of released Cabinet papers or common access point to them.

22.6 A survey conducted by the Cabinet Office in 2004 showed that following release some departments posted the Cabinet paper to their website but this was not common. Occasionally a released paper might be published on the relevant Minister's page on the website www.beehive.govt.nz. There are no common standards on how the Cabinet paper is to be published or displayed.

22.7 Cabinet Office cannot and should not take on the role of deciding on release or releasing papers centrally. This would not fit with the Official Information Act, would take away appropriate decision making by Ministers and departments and would be cumbersome to administer. The current rules for decision making are well established and decisions may be reviewed by the Ombudsman.

22.8 But the question has been raised whether Cabinet Office should become the publisher of record of released Cabinet papers. That has attractions. The decision to release, and the release itself, would remain the responsibility of the relevant Minister or department but the Cabinet Office would publish all released papers on its website. (Departmental websites would have links to the Cabinet Office website.)This would be based on the principle that the Cabinet Office is the central repository of cabinet government records. The central access point would be a single reliable source of what has been released, improve public access to information, and reduce multiple requests for the same information. This is worth considering.

22.9 Care would need to be taken however to ensure that the released version and the published version were the same in that some parts of a paper may have been appropriately deleted before release and indeed those deletions could be the subject of a review by the Ombudsman.

22.10 The Cabinet Office would be likely to need additional resources to administer such a scheme.

22.11 There appears to be scope for more proactive release by Ministers and departments of Cabinet papers of a public policy nature. Many decisions made by Cabinet are in the public arena once the decision is made and public access to the papers would increase public knowledge and reduce Official Information requests. If proactive releases were to increase it would strengthen the argument for the Cabinet Office to be the publisher of record.

22.12 One possibility would be to add to the standard requirements for drafting Cabinet papers a requirement that the paper should discuss whether proactive release would be appropriate and, if so, when. The discussion could identify whether any part of the paper should not be released. A recommendation would then be made for Cabinet to consider. This requirement could be incorporated into the *Step By Step Guide* issued by the Cabinet Office.

Recommendations

Public release of Cabinet Papers

6.1 No change should be made to the current system under which releases of Cabinet papers are the responsibility of the relevant Minister or department.

6.2 The Cabinet Office should consider, in consultation with Ministers and departments, being the publisher of record in respect of all Cabinet papers released

6.3 The Cabinet Office should consider, in consultation with Ministers and departments, extending the standard format of cabinet papers to include a recommendation by Ministers on whether a cabinet paper should be proactively released and, if so, when.

23. List of Recommendations

Terms of Reference Part 1

1.1 Issue the DPMC Security Policy and hold staff briefings on it.
1.2 Prepare a simple guide on the main points for staff to hold.
1.3 Implement the Security Policy and institute compliance checks.
1.4 Reconvene the Interdepartmental Committee on Security to update the "Security in the Government Sector" Manual.

Position (Job) Descriptions

1.5 Standardise the format of position descriptions.
1.6 Ensure that the position description lists the job competencies required.
1.7 Determine the relative importance of each competency by weighting them and use those weightings to assist short listing decisions.
1.8 Include in the position descriptions explanations of the general and any specific responsibilities under the security policy.
1.9 Include in the position descriptions the requirement to be vetted through criminal record checks and, where appropriate, SIS checks.

Selection

1.10 Standardise the format of the write up of appointments.
1.11 Explicitly use the competencies and their weightings in the write up..
1.12 Review the templates used for referee interviews to add to the normal level of questions on honesty deeper questions on the prospective employee's discretion and ethics.

Induction

1.13 Include the proposed simple guide to security policy (see recommendation 1.2) in the induction package

1.14 Redesign the induction checklists to separate out the purely administrative tasks and to document that the substantive tasks have been completed.

Staff Awareness Training

1.15 Design a programme of initial and on going training covering security and related issues and in doing so review the applicability of self-paced on-line training as developed by some government agencies.

1.16 Require Branch Security Officers to keep up to date through training and to schedule regular updates for staff on security issues.

1.17 Consider further ethics training by customising to DPMC needs the State Services Commission's 2003 "Walk the Line" Package.

Corporate Service Resources

1.18 Review the adequacy of the current resources available to the Corporate Services Unit to implement the recommendations in this report.

Terms of Reference Part 2

Pre- Employment Checks

2.1 Extend DPMC pre-employment checks to routinely include criminal record checks through the Ministry of Justice, having obtained the permission of the proposed appointee.

2.2 Extend DPMC pre-employment checks to include financial credit checks, on a case by case basis, with the knowledge of the appointee.

Vetting Requests to the SIS

2.3 Review the levels of security vetting being requested from the SIS to reduce the number of requests and to ensure the vettings requested are commensurate with the level of regular access the employee will have in the future to national security information classified "Confidential" or higher.

2.4 Require employees who are to be vetted by the SIS to bring the completed security questionnaire with them on their first day and actively manage any failure to do so.

2.5 Ensure managers responsible for an employee awaiting SIS vetting are aware of that status so that they may manage access appropriately.

Conflicts of Interest

2.6 Clarify and promulgate the procedural rules surrounding the raising or declaration of conflicts of interest and update the DPMC Code of Conduct

Terms of Reference Part 3

Disposal of Classified Waste

3.1 Review DPMC's contract with the contractor supplying the secure destruction service to include warranties regarding its employees and to specify the standard of shredding to be achieved.

3.2 Review current shredders against the specifications set out in the Protective Security Manual and schedule replacement as necessary.

3.3 Carry out spot checks in line with the DPMC Security Policy to monitor compliance with the disposal policies for classified waste.

3.4 Forward a copy of this report to Ministerial Services and Parliamentary Service to take into account in any review of the other destruction services provided to the parliamentary complex.

Terms of Reference Part 4

Handling of Classified Cabinet Papers in Ministers' Office and departments

4.1 The Cabinet Office should consider incorporating in the Cabinet paper process and in the "Step by Step Guide" a more formal documentation of the classification decision by Ministers' offices or departments. The Guide should also discuss the application of provisional classifications at the policy formulation stage when the paper is being worked up.

4.2 DPMC should develop and issue to Ministerial offices and government agencies a simple guide to the handling, accessing and storage of classified cabinet papers along the lines of the model used by Treasury.

4.3 Cabinet should direct the Cabinet Office to repeat the 2001 instructions that a clear desk policy should be in place in Ministers' offices and in government departments in respect of classified cabinet papers.

4.4 Government organisations should be encouraged to review developments in on-line security awareness training, including reviewing the training packages developed by LINZ and ACC.

Terms of Reference Part 5 – Improvements to Current Classification System

5.1 That a third classification "Highly Sensitive" be introduced for cabinet papers of a public policy or personal privacy nature.

5.2 That the general description and detailed guidelines applicable to the "Highly Sensitive" category, and additional rules for handling, access and storage of them, be drafted with regard to the current principles applying to cabinet papers of a public policy or personal privacy nature.

5.3 That the general description and detailed guidelines of the current two categories " In Confidence" and " Sensitive" be reviewed in conjunction with the new category and in the light of experience since 2001.

5.4 That the "Personal to [Minister]" endorsement be retained and the current rule debarring access by persons other than the Minister be reinforced.

Terms of Reference Part 6- Public Release of Cabinet Papers

Public release of Cabinet Papers

6.1 No change should be made to the current system under which releases of Cabinet papers are the responsibility of the relevant Minister or department.

6.2 The Cabinet Office should consider, in consultation with Ministers and departments, being the publisher of record in respect of all Cabinet papers released.

Proactive Release

6.3 The Cabinet Office should consider, in consultation with Ministers and departments, extending the standard format of cabinet papers to include a recommendation by Ministers on whether a cabinet paper should be proactively released and, if so, when.

24. Acknowledgments

I have received excellent assistance in this review from many people and I thank them for it. A list of people and organisations consulted is at Appendix 4. The conclusions in this report are of course my own. Finally, I thank Becca Darling of the DPMC for her help in putting this report together.

David Henry

Appendices

1. Terms of Reference
2. DPMC Business Units and Functions
3. Cabinet Office Circular CO (01) 10 of 31 July 2001
4. List of People and Organisations Consulted

Terms of Reference Appendix 1

Review of Issues DPMC systems and practices in relation to the handling and security of sensitive information

The State Services Commissioner's report on the investigation of the disclosure of commercially sensitive documents to Telecom earlier this month has recommended that

1. "DPMC considers its policies in relation to practices around the physical collection for disposal of classified documentation in light of the findings of this report and with particular regard to the 'need to know principle'; and

2. DPMC considers steps taken to create copies of classified documentation for media release in light of the findings of this report in order to determine whether any additional policy or communications with Ministers on that issue may be appropriate."

The Chief Executive wants both these recommendations to be pursued as a matter of urgency. In addition he wants to review all of the systems in DPMC that are designed to ensure that sensitive information is handled with the confidentiality and discretion it requires.

The purpose of the review is to ensure all the department's systems are robust and effective going forward in an environment where the trust and confidence of the Prime Minister and Ministers is of the utmost importance.

The review process will involve:

1. Review and identify any areas for improvement in the manner in which DPMC handles its recruitment, selection, induction and staff awareness training procedures.

2. Review and identify any areas for improvement with regard to DPMC's internal security clearance policies and procedures, and staff induction/training and awareness on confidentiality of information and conflict of interest issues.

3. Review and assess DPMC's policies and practices in relation to the secure disposal of classified material.

4. Review and assess whether classified Cabinet papers are being handled, accessed and stored in Ministers' offices, departments and other agencies handling Cabinet material, in accordance with current guidelines; and identify if any improvements to current policies, procedures and guidance are required. *****

5. Review and assess whether the application of the current security classification system is adequate for the protection of highly sensitive Cabinet material (of a public policy nature) and identify if any improvements to the system are required.

   Note:(Items 4 and 5 of the review respond to a Cabinet directive of 8 May 2006 for these matters to be addressed).

6. Review and assess the procedures for providing copies of classified Cabinet papers for public release, following a decision by Ministers to release the material, and consider whether additional policies or guidance should be provided.

7. Recommend any changes to policies and operating procedures as appropriate.

***** This will require consultation with SSC, Treasury and MED and their respective Minister's offices and a small sample –e.g. a large and a small department – of others. It will also involve some consultation with agencies that routinely deal with highly sensitive material.

The review shall be undertaken by David Henry and should be completed by 30 June 2006.

DPMC Business Units and their Functions Appendix 2

1. Cabinet Office (24 staff)

The Cabinet Office is headed by the Secretary of the Cabinet who is also Clerk of the Executive Council. The Secretary/Clerk and her team:

- provide impartial secretariat services to the Executive Council, Cabinet and Cabinet committees
- provide impartial advice to the Governor- General, the Prime Minister and other ministers on certain constitutional and procedural issues, especially those contained in the *Cabinet Manual*
- assist in the coordination of the government's legislative programme
- administer the NZ Royal Honours system
- act as a channel of communication between the Governor-General and government and have responsibility for the overall administration of Government House.

2. Government House (30 staff)

The Government House unit provides administration and support for the Governor-General and maintains Government House and its grounds in Wellington, as well as the smaller Government House in Auckland.

3. Policy Advisory Group (15 staff)

The group:

- Provides impartial advice on issues of the day directly to the Prime Minister and, on occasion, to other Ministers
- coordinates advice coming in from different government departments so that the Prime Minister is given coherent and impartial advice
- contributes to policy development across the full range of government business.

4. Corporate Services Unit (15 staff)

The unit:

- carries out the normal range of corporate functions such as producing the department's Statement of Intent, Annual Report and other accountability documents
- manages human resource capability (for example, recruitment, training, terms and conditions)
- provides financial budgeting, accounting and reporting
- manages information systems.

The Corporate Services Manager is also the department's security officer.

5. Domestic and External Security Group (7 staff)

The group:

- Deals with national security threats that affect New Zealand and its interests, both onshore and offshore
- coordinates the activities of central government action in preparing for and responding to security crises, emergencies and national disasters
- advises the Prime Minister on intelligence and security matters.

6. External Assessments Bureau (29 staff)

The Bureau:

- makes objective assessments of external events and developments using open and classified sources
- produces reports to inform the members of inter-departmental watch groups that coordinate New Zealand's response to external crises and threats to New Zealand.

Appendix 3

Cabinet Office Circular CO (01) 10 of 31 July 2001

Cabinet Office Circular

CO (01) 10

31 July 2001

This document contains information for the New Zealand Cabinet. It must be treated in confidence and handled in accordance with any security classification, or other endorsement. The information can only be released, including under the Official Information Act 1982, by persons with the appropriate authority.

Enquiries:

Martin Bell,…… 4719 740
Margaret Stacey, …. 4719 758

All Ministers
All Chief Executives

Copies to: Speaker of the House of Representatives
Clerk of the House of Representatives
General Manager, Parliamentary Service
Chief Parliamentary Counsel
Controller and Auditor-General
Chief Ombudsman
All Senior Private Secretaries

Revised Security Classifications System: Application to Cabinet Documents

Summary of Key Points

- **Cabinet Office will apply the revised security classifications system to Cabinet documents from 1 August 2001.**

- **It is the responsibility of the originating government department or agency (or Minister's office) to determine the level of security classification applicable to a Cabinet submission in preparation. The classification allocated by the originator will ensure that the submission is given the appropriate level of protection at all stages.**

- **Cabinet submissions containing personal information, such as appointments submissions to the Cabinet Appointments and Honours Committee, should be classified as In Confidence, or Staff: In Confidence, as appropriate.**

- **All departments, Ministers' offices and other government agencies which handle Cabinet documents must ensure that classified Cabinet documents are managed strictly in accordance with the guidelines contained in the Security in Government Departments manual and Addendum 2001.**

- **The minimum handling requirement for Cabinet documents that do not have a specific classification is In Confidence.**

Introduction

1 In December 2000 Cabinet approved a revised system of security classifications for protecting official information. This revised system was promulgated as Addendum 2001 to the Security in Government Departments manual[1]. The revised system is being implemented during 2001/02 after which time compliance will be subject to audit.

2 This circular outlines the application of the revised classification system to Cabinet documents (the term "Cabinet documents" in this circular refers to Cabinet and Cabinet committee agendas, submissions, and minutes. The term "Cabinet submission" means a submission for Cabinet or its committees).

3 Chief Executives and Senior Private Secretaries are responsible for ensuring that:

- all staff involved in the handling of Cabinet documents or preparation of Cabinet submissions are familiar with the advice in this circular;
- the material in this circular is conveyed to all Crown entities or other government agencies for which their Minister is responsible, which are involved in the preparation of Cabinet submissions or the handling of Cabinet documents.

Revised Security Classifications System

4 Under the revised system the security classifications of **Sensitive** and **In Confidence** will be used for information that requires protection for public interest or personal privacy reasons. The existing classifications of **Top Secret**, **Secret** and **Confidential** will continue to be used to protect information concerned with national security, with the addition of **Restricted** as a new national security classification.

5 A summary of the classifications and their applications is set out in the table below[2].

Security Classifications[3]	
Information requiring protection for public interest or personal privacy reasons	
Sensitive	Compromise of information would be likely to damage the interests of the New Zealand government or endanger the safety of its citizens
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
Information requiring protection for national security reasons (ie New Zealand's security, defence, or international relations)	
Top Secret	Compromise of information would damage national interests in an exceptionally grave manner
Secret	Compromise of information would damage national interests in a serious manner
Confidential	Compromise of information would damage national interests in a significant manner
Restricted	Compromise of information would damage national interests in an adverse manner

[1] http://www.security.govt.nz/sigd/addendum/revised.html

[2] Note that Classifications in themselves do not allow official information to be withheld under the Official Information Act 1982. All requests under the Official Information Act must be considered using the criteria in the Act regardless of the classification given to the document concerned

[3] http://www.security.govt.nz/sigd/addendum/classifications

Endorsement Markings

6 A range of endorsement markings[4] may also be used with security classifications to describe the nature of the information being protected. Examples of endorsements used for Cabinet papers are:

Budget: proposed or actual measures for the Budget prior to their announcement

Commercial: sensitive commercial processes, negotiations or affairs

Staff: reference to named or identifiable staff.

7 These endorsements, when combined with a security classification, result in the following examples of classifications and endorsements used for Cabinet papers:

Budget: Sensitive **Commercial: Sensitive**

Commercial: In Confidence **Staff: In Confidence**

Application of Classifications to Cabinet Documents

8 The application of classifications on submissions should be in compliance with the Security in Government Departments manual.

9 It is the responsibility of the originating government department or agency (or Minister's office) to determine the level of classification applicable to a Cabinet submission that they are preparing in order to ensure that the submission receives the appropriate level of protection at all stages of consideration.

10 The revised classifications system means that some of the classifications previously used for Cabinet documents will change. The table below sets out the changes to the main classifications and endorsements currently used for Cabinet documents:

Changes to Commonly Used Classifications and Endorsements for Cabinet Papers[5]	
Previous System	**Revised System**
Budget : Secret	Budget : Sensitive
Commercial : Secret	Commercial : Sensitive
Commercial : In Confidence	Commercial : In Confidence
In Confidence	Sensitive or In Confidence
Staff : In Confidence	Staff : In Confidence
Restricted (this term will now be used as a national security classification (see paragraph 5)	Sensitive or In Confidence (or use a national security classification if appropriate)

11 Consideration should also be given to whether the new classifications of **Sensitive** and **In Confidence** should be used for material not covered by previous classifications.

[4] http://www.security.govt.nz/sigd/addendum/endorsements.html
[5] There are no changes to the current national security classifications of Top Secret, Secret and Confidential

12 All Cabinet submissions containing personal information, such as papers on appointments prepared for the Cabinet Appointments and Honours Committee, should be classified as **In Confidence**. The classification and endorsement **Staff: In Confidence** should be used if the paper concerns information on named staff of an organisation.

13 If a submission is submitted to the Cabinet Office without a classification and it appears that the information in the submission should be classified, the Cabinet Office will assign a classification in consultation with the relevant Minister's office.

Commencement Date

14 The Cabinet Office will commence using the revised classification system for Cabinet documents from **1 August 2001**.

15 The Parliamentary Counsel Office will start using the classification of **In Confidence** for draft bills and regulations from 1 August 2001**,** rather than the classification of Restricted as currently.

16 Treasury has also advised that Cabinet submissions containing information previously classified as Budget: Secret should now use the term **Budget: Sensitive**.

Guidelines for Handling Cabinet Documents

17 Departments and other government agencies handling Cabinet documents are accountable for ensuring the secure handling of Cabinet material in accordance with the protective security principles, and measures for the protection of classified information outlined in the Security in Government Departments manual[6].

18 Each classification has specific guidelines on how the information to be protected should be handled in terms of electronic and paper transmission, storage and disposal. Full details of these updated guidelines have been provided to departments by the State Services Commission (letter to Chief Executives of 12 March 2001).

19 All classified Cabinet documents should be handled in accordance with those guidelines. The minimum handling requirements for Cabinet papers that do not have a specific classification should be those for the classification of **In Confidence.**

20 **Annex 1** of this circular provides a guide to the handling, storage and transmission requirements for classified Cabinet documents. These requirements apply to Cabinet documents at the draft and final stages. The key points are:

- the Cabinet Office delivers Cabinet documents by hand to Ministers' offices.
- Cabinet documents must be transferred securely between Ministers' offices and departments. This means that papers must be enveloped if being delivered by messenger or courier.
- Cabinet submissions being sent by departments to their Minister's office or other departments may be transmitted electronically (ie email) but the information must be encrypted if it is classified as **Sensitive** or has a national security classification.

[6] http://www.security.govt.nz/sigd

- subject to assessment of the risk, submissions classified as **In Confidence** may be transmitted electronically without being encrypted.

- submissions up to the **Sensitive** or **Restricted** level may be sent by facsimile, within New Zealand, on an infrequent basis. Appropriate administrative safeguards should be used to ensure that the intended recipient receives the submission and it is handled securely.

- all Cabinet documents should be kept in secure lockable storage when not in use.

21 Ministers' offices are also reminded that Cabinet documents sent to a Minister outside the parliamentary complex, by VIP Transport or a courier, must be placed in an approved lockable bag.

Further Information

22 For questions or further information about classifications and the handling of Cabinet papers: contact the Cabinet Office Registrar, Margaret Stacey, (phone: 471 9758; email: margaret.stacey@parliament.govt.nz).

23 Further information is available on:

- the revised system for the protection of official information: www.security.govt.nz/sigd/addendum

- minimum protective security principles, and measures for the protection of classified information and related matters – the Security in Government Departments manual, www.security.govt.nz/sigd

Secretary of the Cabinet

Guide to Handling and Transmission Requirements for Classified Cabinet Documents

This table provides a guide to the main handling and transmission requirements for Cabinet documents (ie submissions, minutes and agendas for Cabinet and Cabinet committees) with a classification and endorsement under the revised system for the protection of official information. Full details of the handling, transmission and disposal requirements for classified material are provided in the Security in Government Departments manual, www.security.govt.nz/sigd.

The minimum handling and transmission requirements for Cabinet documents without a specific classification is **In Confidence**.

All Cabinet documents are delivered by hand by the Cabinet Office to Ministers' offices. Documents for Ministers and departments are enveloped by the Cabinet Office when required. It is the responsibility of Ministers' offices to ensure that all Cabinet documents, whether or not they are enveloped by the Cabinet Office, are conveyed securely to their Minister's departments (or other government agencies). All Cabinet documents should be kept in secure storage when not in use.

Classifications/Endorsements for Public Interest and Personal Privacy Reasons

Previous System	Revised System	Paper Transmission	Paper Storage	Electronic Transmission[7]	Electronic Storage
	Sensitive	Must be double enveloped if sending by courier. Cabinet Office delivers papers to Ministers' offices: • unenveloped for Ministers[8] • enveloped for departments	Keep in secure storage when not in use.	Must be marked **Sensitive**. May be transmitted electronically (ie email) only if encrypted[9]. Facsimile systems can be used (within NZ) for infrequent transmission.	Electronic files must be protected against illicit internal use or intrusion by external parties.
Budget Secret	**Budget: Sensitive**	As above	As above	As above	As above
Commercial	**Commercial:**	As above	As above	As above	As above

[7] An originating agency identification, and a confidentiality and privacy statement are required for all information transmitted by email or facsimile.
[8] The Cabinet Office will envelope papers for Ministers that have a "Personal To" endorsement.
[9] The encryption system must be approved by GCSB [eg the SEEmail system].

Previous System	Revised System	Paper Transmission	Paper Storage	Electronic Transmission[7]	Electronic Storage
Secret	**Sensitive**				
In Confidence	**In Confidence**	Must be enveloped if sending by courier. Cabinet Office delivers papers to Ministers' offices: • unenveloped for Ministers • unenveloped for departments	As above	Must be marked **In Confidence**. Subject to risk assessment, may be transmitted electronically (ie email) without being encrypted. Facsimile systems can be used (within New Zealand) for infrequent transmission.	As above
Commercial: In Confidence	**Commercial: In Confidence**	As above	As above	As above	As above
Staff: In Confidence	**Staff: In Confidence**	As above	As above	As above	As above
Restricted [This term will now be used as a national security classification. See below]	Replace with **Sensitive** or **In Confidence** (or use a national security classification if appropriate)	As above for Sensitive or In Confidence	As above	As above for Sensitive or In Confidence.	As above

Classifications for National Security Reasons

Previous System	Revised System	Paper Transmission	Paper Storage	Electronic Transmission	Electronic Storage
Top Secret Secret Confidential	**Top Secret** **Secret** **Confidential**	Must be double enveloped. Can only be conveyed by hand by authorised staff. Cabinet Office delivers papers to Ministers' offices: • enveloped for Ministers (if required) • enveloped for departments	Must be located in approved security container when not in use.[10]	Information transmitted must be encrypted using high grade systems.	Only on systems certified and accredited by GCSB.
	Restricted	Must be double enveloped if sending by courier. Cabinet Office delivers papers to Ministers' offices: • unenveloped for Ministers • enveloped for departments.	Keep in secure storage when not in use.	Must be marked **Restricted**. May be transmitted electronically (ie email) only if encrypted[11]. Facsimile systems can be used (within NZ) for infrequent transmission.	Electronic files must be protected against illicit internal use or intrusion by external parties.

[10] The NZSIS maintains a catalogue of approved equipment.

[11] An originating agency identification and a confidentiality and privacy statement are required for all information transmitted electronically.

Appendix 4

Lists of People and Organisations Consulted

DPMC

Maarten Wevers	Chief Executive
Diane Morcom	Secretary of the Cabinet
Rebecca Kitteridge	Deputy Secretary of the Cabinet
Martin Bell	Deputy Secretary of the Cabinet
Michelle Edgerley	Manager Information and Support Services Cabinet Office
Margaret Stacey	Registrar Cabinet Office
David Baguley	Director Honours Secretariat Cabinet Office
Brent Anderson	Corporate Services Manager
Ronda Sangster	Manager HR and Planning
Shane Beverley	Information Manager
Rachel Goodfellow	HR Adviser
David Jacobs	Head Messenger
Ross Hodges	Messenger
Steve Long	Director DESG
Paul Houliston	Executive Officer DESG
David Kersey	Director EAB
David Hill	Former Director EAB
Don Smith	Manager Support Services Government House
Andrew Kibblewhite	Director, Policy Advisory Group
Dallas Ims	Personal Assistant ,Policy Advisory Group
Anna Whiskin	Information Coordinator, Policy Advisory Group
Donald Clark	Policy Advisor, Policy Advisory Group
Rosemary Cook	Policy Advisor, Policy Advisor Group
Miriama Evans	Policy Advisor, Policy Advisory Group

Ministers' Offices

Heather Simpson	Chief of Staff, Prime Minister
Alec MacLean	Principal Private Secretary, Prime Minister
Kim McKenzie	Senior Private Secretary, Minister of Finance
Gina Anastadiadis	Senior Private Secretary, Minister of Social Development
Beverley Kirbell	Senior Private Secretary, Minister of State Services (MSS)
Jackie Bernstein	Senior Private Secretary (acting), Minister of Economic Development
Bill Moran	Adviser, Minister of Economic Development
Tracy Jamieson	Adviser, Minister of Economic Development
Chris Hipkins	Adviser, Minister of Economic Development

Departments

Geoff Dangerfield	Chief Executive, Ministry of Economic Development (MED)
Alison Nevill	General Manager, Information Management Group, MED
Graeme Carruthers	Deputy Chief Executive, Risk and Assurance, Ministry of Social Development (MSD)
Cathy Sneyd	Chief Security Officer, MSD
Jackie Couchman	GM, Ministerial and Executive Services, MSD
Shenagh Gleisner	Chief Executive, Ministry of Women's Affairs
Martin Sebire	Corporate Support Manager, Ministry of Women's Affairs
Janice Calvert	Acting GM, Executive Government Support, DIA
Richard McDonald	Asst.GM Ministerial Services
Director and officers	SIS
Acting Director and officers	GCSB
Angela Haul-Willis	Deputy Secretary, Treasury
Mark Prebble	State Services Commissioner
Bethia Gibson	Deputy Commissioner, SSC
Simon Murdoch	Chief Executive, Ministry of Foreign Affairs and Trade
Brian Johnston.	Director, Security and Communications Division, Ministry of Foreign Affairs and Trade
Valerie Lambert	Classified Registrar, Ministry of Foreign Affairs and Trade
Joel George	General Manager, Parliamentary Service
John McPadden	Group Manager Operations, Parliamentary Service
David Rudge	National Security Coordinator, Land Information New Zealand
Philip Maitland	General Manager, Financial and Support Services, Ministry of Justice

Other

Julia Kennedy	Manager Support Services, Parliamentary Counsel Office
David Ashton	Management Support Coordinator, Parliamentary Counsel Office
Kevin Brady	Controller and Auditor- General
Deborah Ebbett	Manager e-Learning, Accident Compensation Corporation
Brigid Corcoran	Manager, Law Commission