Australian Government

Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture

Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture

978-1-925363-26-5 Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture (PDF)

978-1-925363-27-2 Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture (DOCX)

Department of the Prime Minister and Cabinet
PO Box 6500
Canberra ACT 2600
Australia
Phone: 02 6271 5111

Dr Martin Parkinson AC PSM
Secretary
Department of the Prime Minister and Cabinet
One National Circuit
Barton ACT 2600

Dear Dr Parkinson,

Following a media report that classified Commonwealth documents had been discovered in secure containers which had been sold to a commercial dealer, you asked me to undertake a review of the security procedures, practices and culture in the Department of the Prime Minister and Cabinet (the Review).

I am pleased to forward to you the attached Report on the Review.

While this Review was necessitated by a particular incident, it is also timely in the context of the broader changes and transformation you have underway across PM&C, including in regard to high-level governance and risk management and to continuing workplace changes in the Department.

I greatly valued the support and contribution of the officers assigned to assist with this Review and the officers I met with who helped inform the Report's findings. Except in regard to the briefing provided by the Department about the incident which triggered the Review, I am of course responsible for the conclusions and recommendations of the Report.

Yours sincerely,

R C Smith AO PSM
23 March 2018

TABLE OF CONTENTS

Review of the Department of the Prime Minister and Cabinet's

security procedures, practices and culture

February 2018

Terms of Reference

INTRODUCTION

At 12 noon on Wednesday 31 January, the ABC published a webpage called "The Cabinet Files". The webpage referenced a series of classified Commonwealth documents provided to the ABC by a third party, reportedly following the purchase of locked filing cabinets at a second-hand furniture shop in Canberra.

The Secretary of the Department of the Prime Minister and Cabinet (PM&C) has referred this matter to the Australian Federal Police (AFP) for investigation into how these documents left the Commonwealth's possession. The Secretary has confirmed that it is reasonably evident that the documents came from within PM&C.

As part of the response to this incident, the Secretary has commissioned Mr Ric Smith AO PSM to undertake an independent review of PM&C's security procedures, practices and culture, including the implications for the Australian Public Service more broadly.

In order for it to effectively discharge its responsibilities, it is critical that the Australian Public Service appropriately safe guards all official information, to ensure its confidentiality, integrity, and availability.

PURPOSE AND SCOPE

The review will make recommendations to ensure that PM&C safeguards official information in an appropriately secure and practical manner that reflects the trust and confidence placed in them by the Government and the Opposition of the day, and will address the implications of these findings for the Australian Public Service.

In particular, the review will consider PM&C's security procedures, practices and culture, including:

- PM&C practices, systems and documented procedures for handling, storing, disposing of and providing access to official information, as well as the safe guarding and disposal of assets used to store official information;
- the effectiveness of these procedures in responding to staff movements and in different working environments; and

- the formal and informal security culture within PM&C, including
    - internal communication and training regarding security, and
    - the awareness, behaviours and attitudes of staff towards proper security.

The review will also address the implications of its findings on these matters for the broader Australian Public Service.

TIMING

It is envisaged that a preliminary Report will be prepared for the Secretary of PM&C by early March 2018, with a final Report by mid-March 2018.

INTRODUCTION

The incident that triggered this Review would have been very serious for any Public Service agency but was especially so for the Department of the Prime Minister and Cabinet (PM&C) given its position at the apex of Commonwealth agencies.

In commissioning this Review, the Secretary of the Department recognised the gravity of the incident and sought advice on measures that needed to be taken to optimise protective security management in the Department.

The incident was investigated by the Australian Federal Police (AFP), whose report identified 'human errors in the record keeping, movement, clearance and disposal of document storage containers by PM&C in 2016 rather than a deliberate unauthorised disclosure'.

This Review concluded that the Department should strengthen the high-level governance of its protective security responsibilities, and demand a more robust security culture in the organisation. While the Department's procedures, protocols and guidelines are generally sound, they are in need of updating and modernising in response *inter alia* to its fast-changing working environment. The shortcomings reflected in the incident which triggered this Review should be addressed through the revision of procedures, protocols and guidelines and through more targeted training programs.

'Protective security' is a term which embraces the security of people, assets, systems, information and documents. Breaches of protective security may arise from activities or failures across a wide spectrum – ranging from espionage to carelessness and error, to assault on individuals, and attacks on property and assets. While the impact of breaches can be especially severe at the level of National Security, the importance of failings at any level should not be underestimated. They can affect government efficiency and inhibit frank consideration of policy or operational options. They can also erode confidence in the Public Service within both the Government and the Opposition, in the Australian community at large and among foreign governments with whom Australia works. Protective security is therefore critical to the functioning of government.

In addressing its Terms of Reference, this Report describes the environment in which protective security must be managed within PM&C (Chapter 1) and then, in order, describes and makes recommendations about:

- the protective security governance arrangements in place in PM&C (Chapter 2),
- the existing documentation in PM&C, including practices, systems and procedures relating to protective security (Chapter 3)
- PM&C's culture in regard to protective security and its relevant training programs (Chapter 4), and
- the implications of the recent incident for the broader Public Service, including lessons that might be drawn from the Review for other agencies (Chapter 5).

.

RECOMMENDATIONS

Chapter One: PM&C's operating environment

1. PM&C's risk management framework should clearly identify the risks associated with the Department's unusually complex operating security environment.

2. As a matter of risk management, all staff joining PM&C at the level of EL2 and above, or promoted to those levels, should be briefed on the complexity of the Department's working environment and the level and nature of the risk they, as managers, are responsible for managing.

3. A further review should be undertaken after 12 months to confirm that the agreed recommendations in this Report have been implemented and, to the extent possible, to measure their effectiveness.

Chapter Two: Protective Security Governance arrangements

4. Protective security should be specified as one of the whole-of-department responsibilities of Deputy Secretary Governance, who should attend the quarterly meetings of the Government Security Committee which is chaired by the Attorney-General's Department, with Deputy Secretary National Security attending National Security related meetings as appropriate.

5. The Executive Board should consider regular, say monthly, compliance or breach reports prepared jointly by the IT Security Advisor (ITSA) and Agency Security Advisor (ASA), including data on breaches and security waivers, recording any incidents of particular concern and explaining the remedial action taken.

6. To facilitate security compliance reporting to the Executive Board, processes for recording security breaches should be improved as soon as practicable to ensure robust security data is collected to enable comparisons over time and between work units.

7. This data should be used to ensure that staff who incur breaches are actively counselled. A staff member who incurs two breaches in a Performance Agreement year should be counselled by a First Assistant Secretary. Three breaches in a year should lead to counselling by the Secretary or Deputy Secretary, and should trigger a review of the staff member's security clearance.

8. In anticipation of a recommendation from a current review of the Protective Security Policy Framework (PSPF), PM&C should nominate the head of Corporate Division as Chief Security Officer, responsible for both ICT and non ICT security.

9. Corporate Division should prioritise the completion of an integrated, real-time framework to link staff profiles and movements (e.g. onboarding, leave, promotion, temporary secondments, and exit) with asset registers including responsibility for individual containers, the assignment of digital devices, and other PM&C records.

10. The 'clear desk' policy required in the Department's Protective Security Plan should be enforced, and security staff clearly mandated to record and report breaches.

Chapter Three: PM&C's documented practices, systems and procedures

11. PM&C's Protective Security Plan (the Plan) and its supporting policies, protocols and guidelines should be updated as a matter of urgency to reflect Machinery of Government changes since 2015, lessons learned from the recent incident, increased digitalisation and changes in office configurations following from the implementation of 'Working Your Way'.

12. The revision of the Plan and its supporting documents should aim for coherency and consistency across the Department's policies and procedures; avoid duplication; ensure that the revised documents are both clear and accessible; and distinguish clearly between those areas in which high-level principles are sufficient and those in which compliance-based directions are necessary.

13. New and specific requirements to the disposal and relocation of security containers should be implemented with immediate effect. Detailed recommendations are set out in the Annex of Chapter 3.

14. Consideration should be given to whether secure containers should simply be destroyed, that is transferred to a scrap metal dealer, with drawers removed, rather than passed to agents for public sale at the end of their useful life.

Chapter Four: Culture, training and behaviours

15. The Secretary and Deputy Secretaries should lead in raising awareness and accountabilities for security across the PM&C network, including by using opportunities in their weekly communication with staff.

16. All Canberra-based new starters should be required to undertake face-to-face security training within the first week of starting at PM&C, including IT security, Physical and Personnel security, and storage and handling of Cabinet documents.

17. All staff in the regional network should be required to complete mandatory online induction training within a week.

18. In parallel, a PM&C team, comprising Learning and Development staff and security personnel, should regularly evaluate the effectiveness of the Department's security training, including assessing the value of face to face training versus e learning modules and training.

19. PM&C's Security section should initiate random but frequent internal security checks, and periodic independent audits of staff security, with an emphasis on the storage of classified information. The outcomes of regular audits should inform targeted areas for further training and nudges.

20. The ASA and the ITSA should consider working with the Behavioural Economics Team of the Australian Government to assess options for increasing security awareness at key points in information and document management processes.

21. The redesign of PM&C's working environments (physical and virtual), including the transition to Working Your Way, must be accompanied by

    a. an assessment of the implications of environmental changes, including the centralisation of key facilities such as shredders and storage facilities;

    b. enhanced promotion of advice for staff accessing PM&C resources on mobile devices in public spaces.

22. Consideration should be given to nominating 'Security Champions' in branches to help grow the security culture and establish a continuous line of communication with the ASA and ITSA.

Chapter Five: Implications for the Australian Public Service

23. Secretaries and agency heads should be advised to review protective security management arrangements in their agencies, paying particular attention to higher level governance and to ensuring an appropriate security culture.

24. In addition to agencies' annual compliance reports, reports resulting from investigations or inquiries into significant security incidents in agencies should be passed to the Attorney-General's Department (AGD), redacted to exclude names and other personal or sensitive information; and AGD should use these reports and the agency compliance reports to develop an annual assessment for the Attorney-General about the 'protective security hygiene' of Commonwealth agencies.

25. AGD should be asked to engage regularly with 'security executives' or ASAs to enable exchanges of information about developments in the area of non-IT protective security and to share 'lessons learned' from any investigations, reports or reviews in the area of protective security.

26. The Australian Signals Directorate (ASD) should be asked to facilitate exchanges of information about cyber security and risk assessments to support greater alignment of risk and planning across agencies.

27. AGD should be asked to survey suitable protective security courses and security training services, including but not limited to courses offered through Registered Training Organisations, and ask agency heads to review the training needs of their staff in this area.

28. Protective security should be routinely included as a standing item on the agenda for Secretaries' Board meetings to enable the Secretary of AGD to report significant incidents and other matters of non-compliance with the PSPF, and to enable the Secretary of PM&C to advise Secretaries on matters relating to agencies' handling of Cabinet documents.

THE INCIDENT AND PM&C's RESPONSE

The following briefing on the incident was provided by PM&C

At 12 noon on 31 January 2018, the ABC published a webpage called "The Cabinet Files". The webpage included a series of articles based on classified Commonwealth documents provided to the ABC by a third party (only some of which were published). The ABC reported that its source found the documents in locked 'filing cabinets' purchased from a second-hand furniture shop in Canberra.

The Secretary of PM&C took immediate steps to:

- refer the matter to the Australian Federal Police (AFP) for investigation into how the documents left the Commonwealth's possession; and
- secure the documents obtained by the ABC and have them returned to the Commonwealth.

On 2 February 2018, the Secretary of PM&C announced that it was reasonably evident the documents came from PM&C, and announced this Review of PM&C's security procedures, practices and culture, including the implications for the Australian Public Service (APS). The Secretary indicated publicly that this was an unacceptable failure and cast the Department in a poor light. The Secretary announced this Review of PM&C's security procedures, practices and culture, including the implications for the Australian Public Service, to help prevent an incident like this from happening again.

How the documents left the Commonwealth's possession

In their report to the Secretary formally responding to the referral of this matter, the AFP confirmed that the classified documents originated from the section responsible for responding to Freedom of Information (FOI) and other access requests within the Cabinet Division of PM&C at One National Circuit, Barton, ACT.

PM&C has confirmed the material obtained by the ABC contained around 300 documents, which were largely collated between mid-2013 and mid-2014 as part of the official business of Cabinet Division (with the majority being working documents relating to FOI and other access requests). While half of the documents were classified Protected or below, there was a small amount of National Security classified material. These documents were not collated for the core purpose of the conduct of Cabinet business nor were they official Cabinet records. They were documents which related to a niche area of Cabinet Division's responsibilities.

The AFP investigation established that the documents are likely to have left the control of PM&C between January and March 2016, following a Cabinet Division accommodation reshuffle in January 2016 when eight secure containers were identified as surplus and returned to Corporate Division.

PM&C has concluded that the secure containers were not checked to ensure they no longer held any documents. PM&C email records indicate that two secure containers in Cabinet Division – formerly used by the officer, or officers, who collated the documents –

were missing keys at the time they were being prepared for disposal. There is no record that the containers were opened and checked prior to disposal.

The (AFP) investigation concluded that 'the catalyst for the documents being made public is attributable to a culmination of human errors in the record keeping, movement, and clearance and disposal of document storage containers by PM&C rather than a deliberate unauthorised disclosure'.

The failings that have been highlighted through examination of PM&C records provided to support the AFP investigation relate to:

- the handling and management of classified information (including copying and storing highly-classified material incorrectly, and retaining working documents beyond their required use); and

- the movement, clearance and disposal of secure containers (including formal tracking of custody of secure containers, clear responsibility for the clearance of locked containers, and management oversight of disposals).

PM&C's response to the incident

In parallel with the investigation undertaken by the AFP and the work of this Review, PM&C has implemented a number of enhancements to existing security arrangements.

- The Secretary and Division Heads have reminded staff of the importance of security and the need to review their own information security practices – both physical and digital. In particular, all staff were required to:

    - immediately re-familiarise themselves with the procedures and policies for the handling of classified information; and

    - examine their filing cabinets, secure containers and personal work areas to ensure classified information was stored properly, or disposed of or returned in accordance with security guidelines.

- PM&C commenced an internal staff security campaign to raise staff awareness of their obligations in relation to physical and digital security, compliance with the Cabinet Handbook, as well as human resources and records management policies.

- The Corporate Division commenced a comprehensive review of their internal security settings to ensure they are fit for purpose and address identified risks. This has included a complete review of secure container handling procedures.

    - New requirements were established for dual sign-off by senior executives in the relevant divisions for any movement of secure containers, and for witnessing procedures on clearance and disposal.

- An audit of all secure containers across the Department was completed.

- All secure containers have also been given a new sequential reference number, and a unique asset identifier barcode and transferred to a digitalised asset register that will record the names of officers with access to the container.

- A new online application (Service Now) process has been implemented to manage requests for new secure containers, their relocation and disposal. This will significantly improve reliability, auditability and tracking of information over the entire life-cycle of secure containers.

- Security section has led several face-to-face tailored security-training sessions for various PM&C work areas.

- New audit and spot check procedures for sensitive and security classified information have been implemented, in accordance with the *Australian Government information security management protocol*.

Secretary Parkinson separately requested counterparts in other agencies to review their own procedures, including auditing their secure containers and any disposals since 2013, and report back to PM&C when this was completed. All Departments of State and relevant PM&C portfolio agencies have complied with this request.

****

Chapter 1: PM&C's OPERATING ENVIRONMENT

This Chapter provides an overview of PM&C's operating environment, highlighting a range of factors that influence the Department's protective security requirements.

PM&C's role

1.1 The role of PM&C is to support the Prime Minister as the Head of the Australian Government and the Cabinet, to provide advice on domestic policy and national security matters, and to improve the lives of Aboriginal and Torres Strait Islander peoples.

1.2 The breadth of the work that is required to support the Prime Minister and the Cabinet is unlike that of other departments and agencies. PM&C encapsulates the functions of every other Commonwealth agency, which increases the diversity of information that must be safeguarded by the Department, and at the same time is responsible for managing the full range of Cabinet processes and documentation.

1.3 To cover the breadth of strategic priorities, the Department has four operational groups which deliver a range of policy and program activities:

a. Domestic Policy Group (Social Policy, Economic, Innovation and Transformation);

b. Governance Group;

c. National Security and International Policy Group; and

d. Indigenous Affairs Group.

PM&C's flexible staffing arrangements

1.4 PM&C operates in a highly flexible manner which is unusual among Public Service agencies. Staff mobility is particularly high. Since 2014, approximately one quarter of PM&C's senior leadership group (e.g. staff at the Senior Executive Service 1 and 2 (SES1 and SES2) levels) has entered or exited the Department in a given year.

1.5 These recent figures align with an earlier August 2012 Capability Review of PM&C which noted the Department's turnover rate in 2010-11 had been approximately 22 per cent for all staff and 30 per cent for SES. The Capability Review noted that turnover was 'a significant risk to future capability' and recommended the 'importance of an effective induction process that introduces new starters to the craft of PM&C and is tailored to level, particularly for SES who do not have central agency experience'.[1]

1.6 This mobility is the product of a number of factors. In general, public servants are encouraged to cycle through the Department rather than make it a career home, and talent and experience are often recruited to particular positions from outside

[1] *Capability Review: Department of the Prime Minister and Cabinet*, August 2012, pages 20-21.

the Public Service in order to inject skills, diversity and experience into the Government's emerging policy work.

1.7 As well, PM&C makes frequent use of taskforces and reviews, often of a multi-agency kind, to develop coordinated whole-of-government responses to emerging issues, or to manage major events and crises. Often stood up at short notice, taskforces and review teams draw on staff from business-as-usual areas of the Department, secondees from other agencies and in some cases contractors who, together, merge various security experiences, cultures and practices. This results in considerable internal staff movement and acting requirements in the Department. In some instances, staff require upgraded clearances or security waivers, additional briefings and training, access to new ICT platforms and the allocation of new physical assets (such as desks and secure containers). (At the time of this Review, there were ten separate taskforces and review teams operating within the Department.)

1.8 Machinery-of Government (MoG) changes also significantly affect the Department. When Indigenous Affairs was brought into the portfolio as part of a range of MoG changes in late 2013, PM&C more than tripled in size from approximately 800 staff to over 2,500 by mid-2014, and significantly expanded its accommodation footprint nationwide.

1.9 Recent changes announced by the Government to Australia's National Security architecture (including the establishment of the Home Affairs portfolio in December 2017) have resulted in further changes to the Department. The Centre for Counter-Terrorism Coordination has now transferred to the Department of Home Affairs, though it remains within One National Circuit (ONC) while appropriate accommodation arrangements are finalised. For the present time, multiple agencies are now collocated within ONC including the Inspector-General of Intelligence and Security, who is expected to transfer to the Attorney-General's portfolio in mid-2018 following the passage of legislation as part of further MoG changes.

PM&C's accommodation footprint

1.10 With three offices in Canberra (ONC, Centraplaza, and Lovett Tower) and a network of Regional Manager Offices and subregional offices within the states and territories, the Department now has some 2,200 staff located in more than 100 locations, and a visiting presence in some 200 other locations across Australia. Security risk and therefore protective requirements vary considerably across these locations, and in some cases within buildings at the same location.

1.11 Within ONC the five floors are divided into five zones with varying degrees of controlled access to designated zones based on business impact levels (for example, National Security areas are spread across Zone 4 and 5 areas, Cabinet Division is in Zone 3, 4 and 5 areas, and domestic policy and corporate functions operate within Zone 3 areas).[2]

[2] A description of Zone definitions is available in the Glossary of Terms in the appendices.

1.12 The creation of taskforces and MoG changes also generate significant office relocations and 'reshuffles', especially in the Barton and Woden buildings. These changes are points of particular vulnerability.

PM&C's transformation agenda

1.13 PM&C continues to embrace innovation and has a strong focus on building a diverse, collaborative, technologically aware, digitally enabled and data-driven workforce. 'Working Your Way', the Digital First/Live Briefing System, and the new online CabNet + viewer (see Box 3) are examples of how PM&C is fundamentally transforming the way it does business. While digitalisation is leading to fewer hard-copy documents in the workplace, it brings heightened risk in other areas.

- Despite the digital transformation underway, PM&C cannot rely on digitalisation of every task it performs to reduce the reliance on paper documentation. Individual preferences, habits and in some cases, Occupational Health and Safety factors, will continue to require classified information to be created, printed and stored in traditional ways.

Security implications

1.14 In managing its security responsibilities amidst transformation and cultural change, it remains critical for PM&C to be able to deal effectively with a mix of 'traditional' protective security requirements and emerging cyber-security related threats. These two areas of risk are in fact intimately connected.

1.15 Following the significant MoG changes in 2013, the achievement of a 'One PM&C' management culture became a high priority for the organisation. It clearly had to be supported by a common level of basic protective security across the organisation as a whole. But the fact that some areas have special requirements relating, for example, to the handling of Cabinet material and material at the highest levels of National Security, leads to a need for stronger security procedures and cultures in some areas than others.

1.16 The challenge here is to establish the minimum basic requirement and to ensure that it is accessible to all while providing tailored and targeted programs for those areas and staff who need them. In effect, the Department is required to manage these higher security 'sub-systems' within its broader security framework.

1.17 Cabinet Division's document and information security 'sub-system' is responsible for the secure handling of Cabinet material both within the Department and across other agencies. With a significant increase in Cabinet business (from 86 Cabinet and Committee meetings in 2006-07 to 157 in 2016-17), and a growing requirement for consultation, the demands on this 'sub-system' are significant.

1.18 The National Security 'sub-system' also embraces a number of features particular to its mandate in regard to intelligence and national security.

1.19 PM&C thus operates in an unusually complex protective security environment, characterised by layered or mosaic-like physical and personnel security requirements and unusually fluid staff management practices. **This is not to excuse any failures that may occur. Rather, it is to emphasise how important it is for all PM&C executives to recognise the nature and scope of the vulnerabilities and risks the Department faces in regard to protective security.**

Recommendations

1. PM&C's risk management framework should clearly identify the risks associated with the Department's unusually complex operating security environment.

2. As a matter of risk management, all staff joining PM&C at the level of EL2 and above, or promoted to those levels, should be briefed on the complexity of the Department's working environment and the level and nature of the risk they, as managers, are responsible for managing.

3. A further review should be undertaken after 12 months to confirm that the agreed recommendations in this Report have been implemented and, to the extent possible, to measure their effectiveness.

Chapter 2: PROTECTIVE SECURITY GOVERNANCE

This Chapter outlines whole-of-government protective security requirements, and describes and makes recommendations about PM&C's governance of its protective security responsibilities.

2.1 Protective security policy for government departments and agencies has long been the responsibility of the Attorney-General's Department (AGD). The Administrative Arrangements Order of 20 December 2017 reconfirmed that responsibility.

2.2 AGD's capstone document guiding Commonwealth agencies in the management of their security responsibilities is the Protective Security Policy Framework (PSPF) (see Box 1). The PSPF was introduced in 2010 with the aim of 'assisting Australian Government entities to protect their people, information and assets, at home and overseas'. The current PSPF was launched by the Attorney-General in October 2014. It is currently being reviewed.

Box 1: The Protective Security Policy Framework

Introduced by AGD in 2010, the PSPF provides a risk-based approach to protective security arrangements for Commonwealth agencies and state and territory government agencies that hold or access Commonwealth security-classified information. The PSPF is largely principles-based, replacing the more prescriptive Protective Security Manual. The PSPF places the onus on individual agencies to develop policies and protocols unique to their own security environment that allow them to carry out the functions of government while safeguarding official resources.

As the Department responsible for protective security policy, AGD collects information on agency performance through annual, self-assessed compliance reporting against 36 core requirements. Reports to Ministers must include a declaration of compliance by the agency head and state areas of non-compliance. Reports are copied to the Secretary of AGD and the Auditor-General. Non-compliance against the mandatory requirements is also reported to the Australian Signals Directorate (ASD) for matters affecting requirements in the Information Security Manual (ISM), and the Australian Security Intelligence Organisation (ASIO) for national security matters.

The PSPF requires agencies to appoint

- a member of the Senior Executive Service (SES) as their 'Security Executive'
- an Agency Security Advisor (ASA) responsible for the day-to-day performance of protective security functions
- an Information Technology Security Advisor (ITSA) to advise on the security of the agency's ICT systems.

In response to the *Independent Review of Whole-of-Government Internal Regulation* by Ms Barbara Belcher AM, AGD is leading significant reforms to the PSPF, to increase protective security policy awareness, simplify requirements and reduce duplication. The 36 principles are currently being redrafted with the intention of reducing them to 16. The revised framework is intended to take effect from 1 July 2018.

2.3 The PSPF requires all Commonwealth agencies to adopt risk management principles and policies appropriate to their functions. Specifically, agencies are required to prepare a security plan to comply with mandatory requirements covering the areas of governance, personnel security, information security and physical security, and to update or revise it every two years or sooner to reflect changes in risks and the agency's operating environment.

2.4 The PSPF is supported by a directive on the 'Security of Government Business', also released by the Attorney-General in October 2014.[3]

2.5 The PSPF is complemented by the ISM, which is produced by ASD (see Box 2).

Box 2: The Information Security Manual

The ISM is the standard which governs the security of government *ICT systems* and complements the PSPF. The ISM is used for the risk-based application of information security controls and provides best practice guidance for making informed risk-based technical and business decisions and implementing strong information security measures. The ISM embraces three complementary documents:

- ISM Executive Companion – details the cyber security threat and introduces considerations for those most senior in an organisation in mitigating the risks presented by this threat environment.
- ISM Principles – details the guiding principles and rationale to assist senior decision makers in developing informed risk-based information security policies within their organisations.
- ISM Controls – details the technical security controls which can be implemented to help mitigate security risks to agencies' information and systems. For example, strategies to mitigate against targeted cyber intrusions, which are outlined in ASD's ISM Controls documentation, must be implemented in order for agencies to be compliant with PSPF mandatory requirements.

The ISM requires agencies to appoint a Chief Information Security Officer (CISO) and that this position is intended to be an agency's Security Executive.

PM&C's Protective Security Management structure

2.6 PM&C is accountable for ensuring the security of people, information, intellectual property, assets, activities and facilities against a range of threats including misuse, loss, damage, disruption, interference, espionage or unauthorised disclosure.

[3] *Securing Government Business: Protective Security Guidance for Executives, Version 2.0*, Australian Government (2014). See https://www.protectivesecurity.gov.au/overarching-guidance/Documents/SecuringGovernmentBusinessProtectiveSecurityGuidanceforExecutivesPrint.pdf

2.7 Responsibility for managing security across this range is shared between the Business Services Branch and the Information Services Branch, both in Corporate Division.

a. The head of the Business Services Branch was named in PM&C's annual PSPF compliance report as the agency 'Security Executive', a designation required under the PSPF. The ASA is an Executive Level 2 position in the Business Services Branch.

b. The head of the Information Services Branch is the Chief Information Security Officer (CISO), a designation required by the ISM. The ITSA, also a position required by the PSPF, is an Executive Level 2 position in the Information Services Branch.

2.8 As noted in Box 2, the ISM specifies that agencies must appoint a CISO who should also be the agencies Security Executive, but the PSPF does not specify that the Security Executive should have the two roles. In PM&C, any uncertainty about the responsibilities of nominated officers could be resolved by designating the head of Corporate Division as the Chief Security Officer (CSO), responsible for both ICT and non-ICT security (see para 2.29 below).

2.9 In terms of reporting, the Business Services Branch briefs the Operations Committee on non-ICT security matters twice a year, normally in March and September. The March briefing is an operational update and an opportunity to introduce new policy or procedures to the Committee for endorsement. The September update is generally used to brief the Committee on the outcomes of the PSPF audit and next steps to rectify non or partial compliance.

2.10 The Information Services Branch provides a report on cyber security operations quarterly to the Operations Committee with a dedicated report on cyber security operational matters. In addition, information on cyber security is provided as input to a monthly Chief Information Officer (CIO) Report.[4] A quarterly report is also provided to the Executive Board with a heightened strategic focus.

2.11 Notwithstanding these two separate lines of reporting, the two branches work closely together and have a good understanding of the interdependence of their respective responsibilities. This is reflected in the PM&C Security Roadmap (2016-2018) and Strategy, approved by the Operations Committee in March 2016, which emphasised that security in PM&C 'is dependent on partnerships with the ITSA, Human Resources (HR) Management and Property Services'.

2.12 As noted, in addition to the security oversight provided by the ASA, the CISO and ITSA, Cabinet Division within PM&C is responsible for managing the Cabinet process across government. This includes the circulation of Cabinet documents in a secure IT system with limited and audited access, tracking distribution of paper copies within PM&C by a barcode identifier, and facilitating distribution of highly-classified documents outside of PM&C by safe-hand. Cabinet Division also undertakes annual stocktakes of hardcopy Cabinet documents held in departments, agencies and ministerial offices. Internally within PM&C, there is a

[4] The head of Information Services Branch is the CIO. The title of CIO is a business title that does not have any specific delegations prescribed in legislation.

biannual stocktake of Cabinet documents. Additional stocktakes occur during caretaker periods.

2.13 Cabinet Division briefs the Secretary of the Department on its stocktake results. Where the number of unfound items is unacceptably high, the Secretary contacts his counterpart in the relevant departments and raises the matter at a monthly meeting of the Secretaries Board. In future, it may also be appropriate to brief the Cabinet Secretary and for Deputy Secretary, Governance to raise any issues at the AGD-chaired Government Security Committee.

PM&C external engagement

2.14 PM&C participates in a number of whole-of-government forums on security matters at various levels. These forums include:

a. The Government Security Committee, chaired at the Deputy Secretary level by AGD. Deputy Secretary National Security currently attends this meeting which meets quarterly;

b. Working level Community of Practice forums hosted by AGD meet periodically in the areas of security culture, ongoing suitability and baseline authorisations; and

c. ASD conducts annual ITSA briefings on current and emerging threats (tailored at both classified and unclassified levels, briefings reflect the various levels of information security across government), as well as regular formal and informal forums for CIOs on cyber-security and information sharing.

2.15 ASD also hosts an annual Australian Cyber Security Centre Conference at which ITSAs network and discuss emerging cyber themes and issues.

Effectiveness of Protective Security Measures

2.16 At a broad level, PM&C's reputation for protective security management has been good, and significant leaks and breaches have been few.

2.17 The Department's protective security performance was audited by an external consultant, Oakton Accounting and Assurance, in August 2015.[5] The audit concluded that PM&C was fully compliant with 31 of the 36 PSPF principles (or 'controls') and partially compliant with the remaining five PSPF principles. The report noted that there were 'no significant security exposures to PM&C as a result of these partially compliant areas, but the Department should continue to progress work currently planned'. The audit made two recommendations:

a. to update security policies and procedures: a review and update of the Agency Security Plan and related policies and protocols be undertaken

[5] *PSPF and Post MoG ICT Security Challenges, Department of the Prime Minister and Cabinet, Internal Audit – 2014/2015*, Oakton Accounting and Assurance.

to ensure all documents are correct and authorised before making final versions available on the intranet; and

b. to ensure compliance with training requirements: PM&C monitor and record when staff are required to complete refresher security awareness training, to ensure compliance with this security requirement.

2.18 In 2016, PM&C's Audit Committee accepted that the recommendations had been implemented.

2.19 Aside from this 2015 audit, there are few metrics currently available for monitoring effectiveness or benchmarking,

a. In regard to the PSPF requirement for an annual compliance report, the Secretary's 2016/17 report to the Prime Minister reported compliance with 32 out of the 36 core requirements.

- Of the four requirements assessed as partially compliant, the majority involved an internal assessment that protective and personnel security plans and policies required updating. While work has progressed on revising these documents, for consistency, they should be captured as part of the broader update of PM&C's Protective Security Plan and supporting policies recommended in Chapter 3 of this Review (Recommendations 11 through 13 refer).

b. As to breaches of security at operational levels within the Department, systems for recording breaches in the ICT domain are relatively robust.

c. Statistics in other areas of protective security are not robust enough to allow detailed interpretation, and monitoring of security compliance is not routinely undertaken. In some cases where a breach is issued, it is not always recorded against an employee if there are considered to be extenuating circumstances.

2.20 The absence of robust metrics may undermine the effectiveness of the Department's Security Breach Notices Policy. This policy (which was last reviewed in October 2016) sets out the arrangements for breaches of protective security requirements, including cases of multiple breaches for staff, contractors and consultants. In short:

a. Staff who incur three security breaches within a performance Agreement year (1 October to 30 September) must provide an explanation to their Division Head and a copy to their Deputy Secretary, Branch Head, Manager and the Security team within two working days.

b. Staff members who incur more than three security breaches may be required to complete mandatory security training, be subject to code of conduct action, have their suitability to retain a clearance questioned or have their security clearance suspended by PM&C pending an Australian Government Security Vetting Agency review.

2.21 This Breach Notices Policy warns that where a formal investigation is undertaken, the staff member's security clearance could be suspended, downgraded or cancelled (subject to appropriate investigations and having due regard for procedural fairness). As a current security clearance is required to access the PM&C Protected Network as well as any of the Department's Canberra buildings, the loss of a security clearance could result in a loss of an essential qualification for employment within the Department.

New Governance

2.22 PM&C's management of its complex protective security environment requires high-level leadership and oversight on a continuous basis.

2.23 The Department's Executive Board is about to put in place new governance arrangements for itself, the Operations Committee, and the People Committee. A new single secretariat will develop integrated work plans for the Executive Board and the People and Operations committees with a focus on ensuring the Secretary has the necessary information to make decisions on the management of the Department. The Executive Board will consider a monthly operations report on finances, human resources and information technology.

2.24 The Audit Committee will continue to run an internal audit program and advise on risk appetite. The Operations Committee will monitor the response to audit recommendations, risk management and risk monitoring. Both committees will report to the Executive Board on audit and risk within the Department.

2.25 Just as the Executive Board will take monthly reports on finance, human resources and information technology, similar reporting should be provided on security breaches, trends and issues, and physical, personnel, ICT and cyber-security related matters. This reporting should include advice to the Secretary about any action considered necessary in regard to counselling recidivist staff through, for example, withdrawal of security clearances or Code of Conduct action.

2.26 Regular reporting to the Executive Board as proposed would enhance oversight of protective security, and confirm it as a significant corporate responsibility as well as a particular responsibility for the Governance Group. This in turn would contribute to strengthening the Department's security culture.

2.27 Whereas Corporate Division is responsible to Deputy Secretary Governance, practice has been for Deputy Secretary National Security to represent PM&C at meetings of the AGD-led Government Security Committee. In the existing structure, Deputy Secretary Governance is responsible for Corporate Division and also for Cabinet Division. To avoid any ambiguity about who is responsible at this level within the Department, Deputy Secretary Governance should represent PM&C on that Committee, reaffirming that position's responsibility for protective security, including Cabinet security, across the Department. Deputy Secretary National Security could of course attend particular meetings if the agenda included items of clear National Security interest.

2.28 In its current review of the PSPF, AGD is expected to require agencies to establish a Chief Security Officer (CSO). The review envisages that, from 1 July 2018, CSOs would be accountable for the security of an agency, embracing informationsecurity, together with personneland physical security, and would become responsible *inter alia* for coordinating responses to security incidents. Changes are also being considered to clarify the roles and accountabilities of agencies which, if adopted, would involve one agency (and the relevant CSO) assuming responsibility for leading security, for example where multiple agencies share a building.

2.29 As noted in para 2.8, it would be appropriate in PM&C for the head of Corporate Division to be designated as CSO. To do this in anticipation of AGD's review of the PSPF would send a strong signal of new governance expectations.

2.30 The Department is also developing a Corporate Master Data Project which will provide an automated end-to-end process for onboarding and offboarding staff, and drive staff compliance in using the correct systems and processes. The process would support changes affecting an individual's pay and conditions, location within PM&C (and temporary movement), training and development needs, responsibilities for PM&C assets (including mobile devices and secure containers), as well as their security records, to be linked (in real time). Such an integrated process would ensure that separate areas within Corporate Division could be notified simultaneously when changing work circumstances might impact on security. The Corporate Master Data Project could deliver on the Department's needs in this regard. In the meantime, the separate Corporate Division processes linked to staff and their movements need to continue to be tightened.

Recommendations

4. Protective security should be specified as one of the whole-of-department responsibilities of Deputy Secretary Governance, who should attend the quarterly meetings of the Government Security Committee which is chaired by the Attorney-General's Department, with Deputy Secretary National Security attending National Security-related meetings as appropriate.

5. The Executive Board should consider regular, say monthly, compliance or breach reports prepared jointly by the IT Security Advisor (ITSA) and Agency Security Advisor (ASA), including data on breaches and security waivers, recording any incidents of particular concern and explaining the remedial action taken.

6. To facilitate security compliance reporting to the Executive Board, processes for recording security breaches should be improved as soon as practicable to ensure robust security data is collected to enable comparisons over time and between work units.

7. This data should be used to ensure that staff who incur breaches are actively counselled. A staff member who incurs two breaches in a Performance Agreement year should be counselled by a First Assistant Secretary. Three

breaches in a year should lead to counselling by the Secretary or Deputy Secretary, and should trigger a review of the staff member's security clearance.

8. In anticipation of a recommendation from a current review of the Protective Security Policy Framework (PSPF), PM&C should nominate the head of Corporate Division as Chief Security Officer, responsible for both ICT and non-ICT security.

9. Corporate Division should prioritise the completion of an integrated, real-time framework to link staff profiles and movements (e.g. onboarding, leave, promotion, temporary secondments, and exit) with asset registers including responsibility for individual containers, the assignment of digital devices, and other PM&C records.

10. The 'clear desk' policy required in the Department's Protective Security Plan should be enforced, and security staff clearly mandated to record and report breaches.[6]

[6] In accordance with paragraph 5.5 of the Department's Protective Security Plan.

Chapter 3: PM&C's DOCUMENTED PRACTICES, SYSTEMS AND PROCEDURES

This Chapter reviews and makes recommendations about the key documented practices, systems and procedures that PM&C has developed to implement its protective security responsibilities.

3.1 PM&C produces, distributes, receives and stores large volumes of classified information created in PM&C and by other Public Service agencies. Handling a wide range of sensitive and classified information is integral to the day-to-day functioning of the Department in its support of the Prime Minister and the Cabinet, and in preparing whole-of-government advice and guidance to the broader APS. The secure handling and appropriate destruction of this information is fundamental to the Government's trust in both the Department and the APS more broadly.

3.2 Managing Cabinet processes and documentation and records is a significant responsibility for PM&C, and imposes particular security and sensitivity requirements. As noted, the volume of Cabinet business, including through the expanded range of Cabinet committees, has increased significantly over the last decade and consultation processes have also broadened – indeed, the online CabNet + viewer has enhanced the accessibility of Cabinet documents.

3.3 This change in the volume of Cabinet business has increased the risk of Cabinet material being misused or mislaid. While the transition to the CabNet + viewer system is helping to mitigate these risks, it also brings new challenges to ensure the security of the environment in which mobile access occurs. There is a continuing need therefore to reinforce both the 'need to know' principle and implementation of the prescribed procedures and processes in relation to Cabinet documents and records.

3.4 Like all government agencies, PM&C is also subject to the *Archives Act 1983,* which imposes obligations for the management of government records.

3.5 PM&C's current Protective Security Plan was drafted in 2015 and last modified in February 2017. It is supplemented by the following guidelines, protocols and policies:

- PM&C Personnel Security Protocol (30 January 2015)
- PM&C Physical Security Protocol (30 January 2015)
- Information Security Protocol (30 January 2015)
- Normal Administrative Practices Policy (28 March 2014)
- Information Management Policy (31 January 2017)
- Records Management Policy (March 2014)
- Classification of Information Guide (11 March 2015)

- Cyber Security: Information and Communications Technology Security Policy (5 February 2018)

- Guidance documents on 'Retention and Destruction of Original Records', and 'How to handle Cabinet Documents'

- Ongoing Suitability Policy (13 December 2017).

3.6 These documents are available online on the Department's intranet with links enabling users to move from one document to another. They are not generally available in hard copy, but can readily be copied (and were for the purpose of this Review). Together with AGD's PSPF, its 'Security of Government Business' directive, the statement on 'Managing Information' in the Australian Public Service Commission's Code of Conduct, and 'The Cabinet Handbook', these documents add up to nearly 300 A-4 pages.

3.7 Printing and collating the full set of these documents highlights both the scope and the cumbersome nature of Departmental guidance on protective security. Though the volume itself may be daunting, the requirements set out are generally very clear and sound. Some of the documents are however dated and differences are evident in the language and style used in the various guidelines, protocols and policies,

3.8 In accordance with the PSPF, the Department's Protective Security Plan should be revised in the light of subsequent MoG changes and other changes in the Department, including increased digitalisation and the introduction of activity-based work practices ('Working Your Way'). At the same time, it would be timely to review the whole suite of subordinate documents with the aim of updating all policies and guidelines and producing a single, coherent, uniformly dated, and more easily accessible package of directions in regard to protective security.

3.9 This is a task which might best be shared between security specialists and a professional editor, addressing not only the content but also the language and overall accessibility of the suite of documents.

3.10 In addition to recommending this revision of the Plan and its associated documents, and while reluctant to add to the existing body of protocols and guidelines, this Review nevertheless offers some specific recommendations in regard to one aspect of document handling, namely, procedures to be followed in relation to the handling of sensitive paper documents when officers move from one work unit to another, or when the documents are no longer required.

3.11 These changes would complement improvements that have been made as part of the digital transformation underway. For example, the new CabNet + viewer offers controlled, but improved and timelier staff access to Cabinet material, while at the same time providing the Department important security enhancements to the way formal Cabinet documents are handled (see also Box 3.)

3.12 The matter of *'safe guarding and disposal of assets used to store official information'*, on which the Terms of Reference sought advice, is not addressed in any documents available to this Review. Again, at the cost of additional bureaucratic compliance, this Review offers some tailored recommendations on this subject.

3.13 During the Review, Security staff confirmed that there is in fact no financial return to the Department from the present disposal practice – while the containers are removed at no cost to the Department, they are not actually bought by the company removing them. Some agencies consign their unwanted secure containers to scrap metal dealers rather than public sales, though it still requires drawers to be open of removed at the point of disposal.

3.14 With regard to *'practices, systems, and documented procedures for handling, storing, disposing of and providing access to official information'*, to which the Terms of Reference refer, these matters are addressed in both the protocols and policies on Information Management and Records Management, and, specifically in relation to Cabinet documents, in The Cabinet Handbook. The Cabinet Handbook was last revised in May 2017. The advice and direction provided relates to both electronic and hard copy documents. Detailed work is underway to further digitalise these processes in regard to Cabinet documents (see Box 3) in an environment in which, as noted elsewhere, the volume of Cabinet business is growing.

Box 3: CabNet+ Viewer

The new CabNet+ viewer is transforming the way Cabinet documents are distributed, shifting away from paper-based circulation to a largely electronic environment. Protected level Cabinet documents (including Exposure Drafts, Drafts, Finals and Minutes) can now be accessed by approved users from any secure device that is connected to an ASD-accredited Protected network. The new system enhances existing security controls around the handling of Cabinet documents, and includes:

- a requirement for the user to agree to the information security terms for accessing Cabinet information;
- a personalised watermark containing the email of the user imposed on the document;
- disabling of print and copy/paste functionality;
- strong system audit controls which allows PM&C's Cabinet Division to monitor and track access to Cabinet documents in any agency; and
- an ability for system Administrators and Coordinators to remove access to Cabinet documents for users at any time – for example, if a staff member transfers into a new position or during a change of government.

While these measures considerably mitigate against the risk of staff storing large volumes of physical Cabinet documents in secure containers unnecessarily, they will not prevent them from creating and storing the associated *working documents* (e.g. drafting suggestions, briefing notes, etc.) outside the CabNet+ viewer and beyond their effective working life.

Recommendations

11. PM&C's Protective Security Plan (the Plan) and its supporting policies, protocols and guidelines should be updated as a matter of urgency to reflect Machinery of Government changes since 2015, lessons learned from the recent incident, increased digitalisation and changes in office configurations following from the implementation of 'Working Your Way'.

12. The revision of the Plan and its supporting documents should aim for coherency and consistency across the Department's policies and procedures; avoid duplication; ensure that the revised documents are both clear and accessible; and distinguish clearly between those areas in which high-level principles are sufficient and those in which compliance-based directions are necessary.

13. New and specific requirements to the disposal and relocation of security containers should be implemented with immediate effect. Detailed recommendations are set out in the Annex of Chapter 3.

14. Consideration should be given to whether secure containers should simply be destroyed, that is transferred to a scrap metal dealer, with drawers removed, rather than passed to agents for public sale at the end of their useful life.

Annex – Disposal and Relocation of Security Containers

In implementing Recommendation 13, the following requirements regarding the management of secure containers should be incorporated in the redrafted Plan and supporting policies and guidelines:

a. Secure containers should not be moved to follow staff when staff move within the Department;

b. Before officers transfer to another division or a section within a division (including a temporary transfer for three months or more), or leave PM&C permanently or for a lengthy period, they must

    i. destroy all working documents under their control that have reached the end of their life in accordance with record keeping policy; or

    ii. formally pass responsibility for remaining documents to another officer.

c. In the event a secure container is to be moved from a Division for any purpose, including disposal, the officer responsible for the container and the ASA should jointly ensure that before the container leaves the Division:

    i. it is unlocked;

    ii. each drawer of a container is open and searched; and

    iii. the key to the empty container remains in the key barrel (for Class C containers) or the electronic lock / spin dial is restored to factory default by the ASA (for Class B containers).

d. If a secure container to be moved for disposal cannot be unlocked prior to leaving the work area:

    i. the Division Head and the Agency Security Advisor (ASA) must authorise the movement of the secure container within PM&C;

    ii. the Division Head (or an officer delegated from within the Division) and the ASA are physically present for the movement of the secure container and the steps at (c) must be performed before responsibility for the container is formally handed to the ASA;

    iii. if the movement of the secure container and the steps at (c) cannot be performed at the same time, then the ASA should accept temporary responsibility until the Division Head (or delegate) and the ASA are present to oversee the steps in (c).

e. Before a secure container leaves PM&C, the ASA should:

    i. ensure that it is unlocked;

ii. ensure each drawer of a Class B container is pulled open and the area behind the drawer is searched (and the area at the bottom of a Class C container is searched); and

iii. ensure the key to the empty container is in the key barrel (for Class C containers) or the electronic lock / spin dial is set at factory default (for Class B containers).

f. A register of all secure containers be established (or resurrected) and kept current, recording the officer(s) and the relevant manager of the division as the persons responsible for that secure container and its contents.[7]

g. The preparation and disposal of secure containers be overseen by the ASA, and receipts obtained from the buyer, or the destruction facility to which they are being consigned, confirming that the secure containers received are open and empty.

h. Secure containers removed from PM&C should be fixed with a discrete indicator confirming the Department of origin.

[7] In train as of 8 March 2018.

Chapter 4: CULTURE, TRAINING AND BEHAVIOURS

This Chapter addresses the matter of security culture within PM&C, corporate communication on the subject and Departmental training programs, and offers recommendations for change.

Culture

4.1 Previous Chapters have commented on aspects of PM&C's security culture. This Review was not able to survey attitudes across the Department, but did reach some broad conclusions which were supported by senior officers with experience of the organisation.

4.2 The Review was presented with no evidence to challenge the view of one senior officer that 'the great majority (of staff) intend to do the right thing and largely are left to do it instinctively'. It was also noted that there has not been a significant 'leak' from the Department since 2001.

4.3 Clearly, while all staff must understand basic physical security and document handling requirements, those who have a close involvement with National Security matters or come to the Department from agencies within the National Security community have a stronger understanding of their security obligations and are experienced in managing them.

4.4 That said, failures in protective security practice undoubtedly occur. Under the pressure of time and work-place demands, staff almost certainly adopt 'work-arounds' at times and behaviours can fall below required standards. As previously explained, the data available from physical security breach records does not enable a detailed analysis of practices in regard to non-ICT security across the Department but the breaches that are recorded indicated a need for continuing rigorous implementation of the existing protocols and guidance.

4.5 To minimise the risks of security failures either deliberately motivated or of a kind arising from carelessness or human error, PM&C should ensure that its culture is one that deters 'excusable behaviour' and rewards 'accountable behaviour' and recognises that 'security is everyone's everyday business'.

4.6 A positive culture of this kind could be fostered by a combination of measures proposed in this Report. Foremost of these is a stronger, more leadership-driven governance regime (as proposed in Chapter 2). The revision of Departmental security protocols and guidelines (as proposed in Chapter 3) and their firm application, and more targeted training as described below, will also help foster a stronger culture.

Training

4.7 The Department's Protective Security Plan sets out requirements for all staff to complete security training at induction and then annually as part of refresher training. In practice, PM&C staff (including ongoing, non-ongoing and secondees) and contractors required to access the building must complete online security induction training within three months of commencement. This induction

includes basic security information targeted at the baseline level and is done via an online interactive LearnHub course. While this online training module ensures compliance, is low cost, and is accessible to the broader PM&C network, the overall effectiveness has not been evaluated by PM&C's Security or Learning and Development teams.

4.8 In response to the recent security incident, face-to-face security training was introduced in February 2018 to complement the online interactive LearnHub course. Staff based in Canberra (who generally have access to higher classified material) now have the option to complete the mandatory security training either online or in a face-to-face environment. In addition, staff who receive multiple security breach notifications are also required to attend face-to-face training. Attendance is monitored through PM&C's Learning and Development portal, with non-compliance followed up with employees and their supervisors.

4.9 While PM&C's graduate intake is provided at induction with a comprehensive training program, which includes security training, other new starters at PM&C have historically been dependent on a series of online training modules accessed through the Department's intranet. Targeted face-to-face induction training for all Canberra-based staff that covers IT Security, Physical and Personnel Security and the storage and handling of Cabinet documents is likely to be more effective.

4.10 The Security section also provides tailored security briefings to individual work areas on request.

4.11 Within its own security sub-system, Cabinet Division manages a range of training processes to build awareness of the Cabinet process both within PM&C and across the Public Service. These processes include:

a. a course on 'Producing a Quality Cabinet submission' in partnership with the Australian Public Service Commission;

b. workshops and presentations with the Cabinet Liaison Officer Network across the APS;

c. targeted briefings and presentations to departments/agencies on the Cabinet process;

d. ad-hoc presentations to staff in Ministers' Offices on the Cabinet process;

e. engagement with staff in policy line areas in PM&C and with drafters in other departments;

f. training for users of CabNet+ Viewer (a mix of face to face and video training); and

g. distribution of Cabinet Circulars.

4.12 Noting the significance of the Cabinet Division's work within PM&C (and its importance under the *Archives Act 1983*), high-level induction training should be provided for Canberra-based new starters on Cabinet processes (including the secure handling and storage of Cabinet documents, and the importance of the 'need to know' principle). Cabinet Division should also of course continue to provide training and guidance on Cabinet processes for staff in Ministers' Offices.

Behaviours

4.13 Documented procedures, together with effective security training, underpin a common understanding among staff about the environment in which they operate. Documented responsibilities not only establish clear accountabilities but also support consistency and reduce the risk of ad-hoc security arrangements being applied across organisations.

4.14 No amount of documentation can however be guaranteed to eliminate human error. To minimise the risk of security-related incidents, PM&C's response must go further than simply reviewing, improving and applying documented policies and rules and mandating training in response to the current incident.

4.15 In a similar way that behavioural insights are being used to improve policy design and outcomes, they could be expected to improve security compliance.

Understanding staff behaviours

4.16 While security needs to be everyone's everyday responsibility, PM&C has to make it easy for staff to comply. Not every staff member will read every paragraph of the security documentation or be able to recall the detailed security requirements during periods of peak activity.

4.17 When overwhelmed with information, individuals – either consciously or sub-consciously – rely on short-cuts or rules-of-thumb. By carefully observing these choices, it should be possible to shape more realistic models of human behaviour and to develop targeted 'nudges' to influence choices and improve policy outcomes.

4.18 PM&C's Security section could thus look to behavioural insights and innovative solutions to help staff with compliance. For example, 'pop-ups' could offer staff tips on how to classify and store a document when a file is created or saved, and shredding reminders could be appear when staff print material. These simple steps provide the first line of security defence.

4.19 The Department also needs to be mindful of how changes in the physical environment could impact on compliance. Changes that inadvertently lead to security workarounds to enable staff 'to get the job done' can result in individuals taking actions outside of the established security procedures and practices.[8] For instance, the consolidation of shredders and secure containers could make it more time-consuming for staff to comply.

[8] "When policies and mechanisms demand too much effort, and when the effort becomes unreasonable, humans make mistakes or cease to comply". Kirlappos, I, Parkin, S and M. A Sasse, *Learning from Shadow*

4.20 To effectively mitigate against future security incidents, PM&C cannot rely on a single solution. In particular, relying on centrally-driven approaches (e.g. revised arrangements for moving secure containers) runs the risk of staff becoming complacent about their security responsibilities and instead relying on others to manage security outcomes. Moreover, the tools that might be useful in improving individual behaviours today could be different to those that work in the future and so continuous improvements in the security culture will require ongoing evaluation (of training) and observation of behaviours (via health checks and reporting) to ensure PM&C understands what tools work.

4.21 It was suggested to the Review that, to improve the overall security consciousness in the Department, 'Security Champions' could be nominated to create a line of communication between the PM&C Security section and branches. 'Champions' would not be responsible for policing Branch breaches or incidents but, rather, would provide on-the-ground reminders and disseminate simple and timely hints to heighten awareness during peak work periods. 'Champions' could also help to raise staff awareness on the use of mobile devices, a matter on which some staff are uncertain.

Recommendations

15. The Secretary and Deputy Secretaries should lead in raising awareness and accountabilities for security across the PM&C network, including by using opportunities in their weekly communication with staff.

16. All Canberra-based new starters should be required to undertake face-to-face security training within the first week of starting at PM&C, including IT security, Physical and Personnel security, and storage and handling of Cabinet documents.

17. All staff in the regional network should be required to complete mandatory online induction training within a week.

18. In parallel, a PM&C team, comprising Learning and Development staff and security personnel, should regularly evaluate the effectiveness of the Department's security training, including assessing the value of face-to-face training versus e-learning modules and training.

19. PM&C's Security section should initiate random but frequent internal security checks, and periodic independent audits of staff security, with an emphasis on the storage of classified information. The outcomes of regular audits should inform targeted areas for further training and nudges.

20. The ASA and the ITSA should consider working with the Behavioural Economics Team of the Australian Government to assess options for increasing security awareness at key points in information and document management processes.

Security – why understanding non-compliant behaviours provides the basis for effective security, Department of Computer Science, University College of London, London, United Kingdom.

21. The redesign of PM&C's working environments (physical and virtual), including the transition to Working Your Way, must be accompanied by

    a. an assessment of the implications of environmental changes, including the centralisation of key facilities such as shredders and storage facilities; and

    b. enhanced promotion of advice for staff accessing PM&C resources on mobile devices in public spaces.

22. Consideration should be given to nominating 'Security Champions' in branches to help grow the security culture and establish a continuous line of communication with the ASA and ITSA.

Chapter 5: IMPLICATIONS FOR AUSTRALIAN PUBLIC SERVICE AGENCIES

This Chapter considers the implications of the findings of this Review for the broader Australian Public Service and recommends service-wide responses.

5.1 Failings of the kind that gave rise to the incident which triggered this Review have occurred in other departments and agencies, and are potentially systemic in the Public Service. This latest incident should be a 'wake-up call' for all agencies. Secretaries and Chief Executive Officers should be advised to check the recommendations of this Review against protective security management in their organisation. This applies especially to matters of corporate governance and culture.

5.2 As noted in Chapter 2, in accordance with the Administrative Arrangements Order, AGD has policy responsibility for protective security among Commonwealth agencies and has set out its guidance to agencies in the PSPF. As further noted in Chapter 2, AGD's role is supported by the work of ASD. Indeed, the PSPF requires agencies to implement strategies contained in ASD's ISM in order to be compliant with the PSPF. The thinking behind the risk and principles-based PSPF was that departments and agencies knew their own workforces, workplaces and risks best and should develop and take responsibility for their own agency-specific policies, procedures and protocols.

5.3 As noted earlier, AGD chairs a Government Security Committee which meets four times a year at the level of Deputy Secretary with a mandate *inter alia* to 'provide strategic oversight of whole-of-government protective security policy'. It also convenes a number Community of Practice (CoP) meetings at different levels.

5.4 AGD receives copies of the compliance reports which agencies submit annually to their Ministers, provides benchmarking information to reporting agencies, identifies high-risk agencies, and offers some better practice guidance but it does not maintain a view of 'security hygiene' across the Commonwealth, or serve as a 'clearance house' for 'lessons learned' among agencies, or advise on practical examples of best practice among agencies. A more active role by AGD in advising this area could be expected to benefit protective security management within the Australian Public Service.

5.5 ASD and ASIO, as technical authorities, provide advice and support to Commonwealth agencies on protective security-related matters. In particular:

a. The ASD has a formal agency-wide role in relation to ICT and cyber security. Departments are required by the PSPF to report to ASD any incidents of non-compliance with the Information Security Manual (ISM). ASD also provides guidance to help organisations assess security vulnerabilities, including the risks posed if security patches are not applied in a timely manner. Any lessons learned are currently shared on an ad-hoc basis.

b. ASIO also has a role among agencies, albeit their role is less well-defined than that of ASD. ASIO provides advice about any significant changes in threat levels, advises on technical and compliance standards of

equipment or technology, and also delivers training courses on some aspects of security, for example, managing Security Zones. ASIO also issues security newsletters to update ASA's and remind them of appropriate practices. Its level of engagement with agency ASAs beyond this is however uneven.

5.6 As noted previously in paragraph 2.14, networking among agency personnel involved in protective security also varies.

a. There appears to be an effective CIO and ITSA network across central agencies. Departmental ITSAs meet informally every few months to discuss issues and provide points of contact; in the meantime they are well-networked and for instance exchange data about the frequency and nature of incidents affecting their systems.

b. The same degree of 'connectedness' and information sharing is not evident at this time in regard to non-ICT related protective security. There is some exchange at an informal level, but for instance lessons or recommendations arising from enquiries or investigations into incidents are not shared among agencies (or received by AGD).

5.7 The Review heard a number of references to the difficulty of recruiting adequately trained staff for roles in security areas in government agencies, especially ASAs in smaller agencies. This challenge was said to have grown since the closure in 2017 of the Protective Security Training College (formerly managed by AGD) after suitable courses were established by external registered training organisations (RTOs). It was said however that the government focus at RTO courses had diminished in favour of commercial and industrial security training, and that the costs of courses had also increased. It could be timely to draw this matter to the attention of AGD and Public Service agency heads.

5.8 Noting the importance of protective security to the efficient functions of government, it would be timely to introduce consideration of protective security issues as a standing item on agenda of the Secretaries Board.

Recommendations

23. Secretaries and agency heads should be advised to review protective security management arrangements in their agencies, paying particular attention to higher-level governance and to ensuring an appropriate security culture.

24. In addition to agencies' annual compliance reports, reports resulting from investigations or inquiries into significant security incidents in agencies should be passed to the Attorney-General's Department (AGD), redacted to exclude names and other personal or sensitive information; and AGD should use these reports and the agency compliance reports to develop an annual assessment for the Attorney-General about the 'protective security hygiene' of Commonwealth agencies.

25. AGD should be asked to engage regularly with 'security executives' or ASAs to enable exchanges of information about developments in the area of non-IT protective security and to share 'lessons learned' from any investigations, reports or reviews in the area of protective security.

26. The Australian Signals Directorate (ASD) should be asked to facilitate exchanges of information about cyber security and risk assessments to support greater alignment of risk and planning across agencies.

27. AGD should be asked to survey suitable protective security courses and security training services, including but not limited to courses offered through Registered Training Organisations, and ask agency heads to review the training needs of their staff in this area.

28. Protective security should be routinely included as a standing item on the agenda for Secretaries' Board meetings to enable the Secretary of AGD to report significant incidents and other matters of non-compliance with the PSPF, and to enable the Secretary of PM&C to advise Secretaries on matters relating to agencies' handling of Cabinet documents.

APPENDICES

APPENDIX A – The Review Team

The Independent Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture was led by Mr Richard Smith AO PSM with the support of a secretariat drawn from PM&C.

The views expressed in this Review are those of the author.

Methodology

The Review was to follow an investigation of the incident by the Australian Federal Police (AFP). In order to meet the Terms of Reference timeframes, work commenced before the AFP Report was finalised. Care was taken to separate the work of the Review from that of the AFP. In particular, the Secretariat made clear to the individuals interviewed that the Review was not to duplicate the investigation, or to make assumptions about responsibility for the incident.

In conducting this Review and to ensure a whole of Department perspective, meetings were held with officers of varying levels from all four work streams within PM&C- Governance Group, National Security and International Policy Group, Domestic Policy Group and Indigenous Affairs Group. These discussions proved valuable in understanding the breadth of PM&C's responsibilities, and provided opportunities for officers to share their observations of PM&C's security procedures, practices and culture. In the context of the fluid staff movements of the Department, some officers were usefully able to offer observations and comparisons from their experiences in other Commonwealth departments.

In addition, some meetings were held with external agencies, including the. Attorney-General's Department, the Australian Security Intelligence Organisation, the National Archives of Australia and the Treasury. Contact was also made with the Australian Public Service Commission and the Department of Defence.

Careful consideration was given to the various documented policies, protocols and guidelines that govern PM&C's information security requirements.

Although time did not permit more comprehensive engagement across the PM&C network, that is, in the states and territories, the success of many of the recommendations in this Review will be conditional on the feedback from PM&C staff at all levels, and across the organisation.

APPENDIX B – Meetings – internal

Department of the Prime Minister and Cabinet	
Stephanie Foster Deputy Secretary	Governance
Yael Cass First Assistant Secretary	Cabinet Division
Michele Graham Assistant Secretary	Cabinet Division
Nathan Bird Project Manager	CabNet Redevelopment project
Senior Advisor	CabNet Redevelopment project
Project Officer	CabNet Redevelopment project
Charlotte Tressler First Assistant Secretary	Corporate Division
Pat Sowry Assistant Secretary	Business Services Branch
Agency Security Advisor	Business Services Branch
Nathan Heeney Chief Information Officer	Information Services Branch
IT Security Advisor	Information Services Branch
Emma Greenwood Assistant Secretary	People Branch
Advisor	People Branch
Allan McKinnon Deputy Secretary	National Security and International Policy
Kylie Bryant First Assistant Secretary	National Security Division
Lee Walton First Assistant Secretary	Information Sharing and Intelligence Division
Chris Angus Assistant Secretary	Intelligence Branch
Trevor Jones Assistant Secretary	Home Affairs Branch
Advisor/Intelligence Distribution Officer	Home Affairs Branch
Lin Hatfield-Dodds Deputy Secretary	Domestic Policy - Social

Department of the Prime Minister and Cabinet	
Barry Sterland Deputy Secretary	Domestic Policy -Innovation and Transformation
David Gruen Deputy Secretary	Domestic Policy - Economic
Tanja Cvijanovic First Assistant Secretary	Policy Innovation and Projects Division
Tara Oliver Managing Director	Behavioural Economics Team of the Australian Government (BETA)
Bob Slonim Research Director	BETA
Andrew Tongue Associate Secretary	Indigenous Affairs
Ian Anderson Deputy Secretary	Indigenous Affairs
Jamie Fox First Assistant Secretary	Indigenous Employment and Recognition Division
Deborah Lewis First Assistant Secretary	Community and Economic Development Division
Rachel O'Connor Assistant Secretary	Policy, Analysis and Evaluation Division

Meetings – external stakeholder engagement

External stakeholder engagement	
Chris Moraitis Secretary	Attorney-General's Department (AGD)
Sarah Chidgey A/g Deputy Secretary	Criminal Justice and National Security, AGD
Anna Harmer First Assistant Secretary	Security and Criminal Law Division, AGD
Director	Protective Security and Fraud Policy, AGD
David Fricker Director-General	National Archives of Australia
Teresa Ward Assistant Director-General	National Archives of Australia
Duncan Lewis Director-General (and others)	Australian Security Intelligence Organisation
Chief Security Officer	The Treasury

APPENDIX C – Glossary of terms

Term	Definition
Baseline security clearance	Security clearance required for ongoing access to security classified information at the PROTECTED level, or where a level of assurance is required of a person's suitability to perform a role.
CabNet	Whole-of-Government IT system that facilitates the management, storage and distribution of Cabinet information.
CabNet+ viewer	Read-only viewing and distribution of Protected Cabinet documents on desktop and mobile devices on Protected networks.
Class B secure container	A secure container manufactured to ASIO-approved specifications that uses an electronic combination lock.
Class C secure container	A secure container manufactured to ASIO-approved specifications that uses a cam lock (Bilock key).
Clear desk policy	A policy requiring a person to ensure that official information and other valuable resources are secured appropriately when the person is absent from their workstation of work place.
Digital First (paper lite)	Information and services designed in the online environment for consumption via a digital medium.
Information Security Manual (ISM)	The Australian Government Information Security Manual, produced by the Australian Signals Directorate, is the standard which governs the security of government ICT systems. It complements the Protective Security Policy Framework.
LearnHub	PM&C's online learning management system.
Live Briefing System	Browser application used to create, draft, track workflow, and present briefings to the Prime Minister's Office.
Machinery of Government (MoG) changes	Change in structure of government agencies across the public sector.
Registered Training Organisation (RTO)	Providers and assessors of nationally recognised training.
Security Breach	An accidental or unintentional failure to observe the protective security mandatory requirements.

Term	Definition
Security Incident	A deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of official resources.
Security Zones	A method of assessing the security of areas used for protecting people, or handling and storing information and physical assets based on security controls.
Security Zone One	Unsecured areas including out of the office working arrangements.
Security Zone Two	Low security area with some controls and access control for visitors.
Security Zone Three	Security area with higher level security controls than Security Zone Two, strict control of visitors on a needs basis and access to employees controlled.
Security Zone Four	Security area with higher level of controls than Security Zone Three, and strict visitor and employee access controls on a needs basis.
Security Zone Five	Security area with the highest level of controls, strict visitor and employee access controls on a needs basis.
Service Now	PM&Cs online service management tool for IT, Human Resources, Communications, Facilities, IAG Grants Administration and Security.
Working Your Way	An initiative to improve PM&C's working environment, integrating physical settings with modern technology to change the way we work and harness innovation.