Australian Government
Department of the Prime Minister and Cabinet

Report to the Department of the Prime Minister and Cabinet

on

Implementation of the 'Smith Review' and progress in strengthening protective security procedures, practices and culture: 12 month follow-up review

Review undertaken and report prepared by Mr Peter Vardos PSM

June 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

INTRODUCTION 4

THE SMITH REVIEW RECOMMENTDATIONS 4

METHODOLOGY 5

OVERVIEW 5

THE DEPARTMENT OF THE PRIME MINISTER AND CABINET 7

ATTORNEY GENERAL'S DEPARTMENT 10

AUSTRALIAN SIGNALS DIRECTORATE 10

THE WIDER APS 11

LESSONS FOR ALL 12

ATTACHMENTS 14

Executive Summary

The response of the Secretary of the Department of the Prime Minister and Cabinet (PM&C) to the *Cabinet Files* incident of January 2018 was swift and comprehensive. The ensuing Smith Review and its associated report containing 28 recommendations addressed a range of protective security issues which went beyond the physical storage, handling and disposal of sensitive government documents. The Smith Review recommended, *inter alia*, that a further review be undertaken after 12 months to confirm that the agreed recommendations were implemented and, to the extent possible, to measure their effectiveness.

At the time this 12 month follow-up review report was submitted to PM&C all 28 recommendations had been actioned by the three responsible agencies, namely PM&C, the Attorney-General's Department (AGD) and the Australian Signals Directorate (ASD). Eight recommendations had been completed and 20 recommendations had been completed but with a long term implementation aspect.

Significant steps have been taken by PM&C to give protective security a higher posture in the organisation. The current protective security framework is comprehensive and visible to staff. Staff are sensitised to the need to understand the reasons for maintaining high standards of protective security. This is driven in large part by the lingering memory of the events of January 2018 and the fallout for the Department. However, with the high rate of staff turnover in PM&C, the recollection of the impact of the *Cabinet Files* incident will wane, as will its role as a driver for staff to maintain their focus, vigilance and enthusiasm for protective security. The challenge remains for PM&C's leadership to maintain strong messaging and staff focus on an ongoing basis on the need for high standards of protective security.

The lessons from the *Cabinet Files* incident and the Smith Review resonated across the Australian Public Service (APS). They have acted as a catalyst for reviewing and upgrading internal protective security policies and procedures. In some instances, protective security initiatives were already under way but received greater attention and priority as a consequence of those events.

Agencies which operate outside the general environment of security, intelligence and law enforcement, and which do not regularly handle highly classified information, face a particular challenge in maintaining staff focus on protective security best practice. Similarly, officers appointed to the role of Chief Security Officer (CSO) in those agencies can lack the experience and professional expertise to properly undertake those roles. AGD and ASD have a critical role in providing coordinated and comprehensive support to assist CSOs to meet their responsibilities.

1. INTRODUCTION

1.1 On 31 January 2018, the ABC published a webpage called *The Cabinet Files*. This covered a series of articles based on Commonwealth documents provided to the ABC by a third party. The ABC reported that the documents had been located in locked, ex-government filing cabinets which had been purchased by a private citizen from a second-hand furniture dealer in Canberra.

1.2 The Secretary of the Department of the Prime Minister and Cabinet (PM&C) took immediate action which, inter alia, included:

- referral of the matter to the Australian Federal Police (AFP) for investigation;
- securing the documents which were in the possession of the ABC;
- commissioning Mr Ric Smith AO PSM to conduct a comprehensive review (the Smith Review) of the events that led to the documents leaving the possession of the Commonwealth Government;
- launching an SES-led communication campaign with PM&C staff in relation to security procedures and the handling of sensitive and privileged information;
- an audit of all secure containers in PM&C;
- initiating a structured change process in PM&C in relation to security procedures, practices and culture;
- engaging with his counterparts in other agencies to request them to review their own security related procedures and to report back to PM&C.

1.3 The Smith Review report was submitted to the Secretary of PM&C on 23 March 2018. It contained 28 Recommendations covering: PM&C's operating environment; Protective Security governance arrangements; PM&C's documented practices, systems and procedures; culture, training and behaviours; and implications for the Australian Public Service (APS).

2. THE SMITH REVIEW RECOMMENDATIONS

2.1 The essence of the Smith Review recommendations can be broadly summarised as:

- the clear identification and management of risk in the PM&C in the handling, storage and disposal of sensitive documents/privileged information;
- personal accountability of staff for protective security;
- clearly defined and promulgated policies for protective security;
- clearly defined and promulgated policies and operational processes for the disposal of security containers;
- staff training and awareness-raising to equip staff to do what is expected of them with respect to protective security and the handling of sensitive documents/privileged information;
- compliance monitoring and reporting;
- outreach to other APS agencies to engender a cooperative, whole-of-APS approach to protective security.

2.2 The full Terms of Reference for the Smith Review are at **Attachment 1.**

2.3 Recommendation 3 of the Smith Review stated:

> *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.*

3. METHODOLOGY

3.1 The follow-up review was undertaken by Mr Peter Vardos PSM, with support drawn from Security and Business Support Branch, PM&C. The Terms of Reference for the 12 month follow-up review are at **Attachment 2.**

3.2 I met with a range of senior officers in PM&C who were involved with the implementation of the Smith Review recommendations or whose business practices have been impacted by the implementation of the recommendations.

3.3 I reviewed the body of work produced and underway, in response to the Smith Review recommendations, under the stewardship of Security and Business Support Branch

3.4 I chaired focus group discussions with a representative sample of more junior officers from across PM&C.

3.5 I met with officers from the Attorney General's Department (AGD) and the Australian Signals Directorate (ASD), agencies which were directly referenced in the Smith Review. My objective was to ascertain the extent to which the Smith Review recommendations that focused on these agencies had been implemented.

3.6 I met with a number of Chief Security Officer's (CSO's) from mid-sized to large agencies that generally operate outside the security, intelligence and law enforcement sphere. My objective was to ascertain the extent to which the consequences of the *Cabinet Files* incident and the recommendations of the Smith Review impacted on a sample of departments outside the security fraternity.

3.7 I met with the CSO of the Department of Home Affairs (Home Affairs). My objective was to determine the extent to which an agency that operates in the security, intelligence and law enforcement environment was impacted by the *Cabinet Files* incident and the recommendations of the Smith Review.

4. OVERVIEW

4.1 The Assistant Secretary, Security and Business Support Branch (SBS), Corporate Division, PM&C was tasked with overseeing the implementation of the recommendations of the Smith Review. The officer occupying that position was specifically recruited by PM&C to take forward the recommendations. In the ensuing 12 months, substantial progress has been made in the implementation of all recommendations.

4.2 As at June 2019, when the report of the follow-up review was submitted, there were no recommendations which remained unactioned. In summary: seven recommendations were completed prior to the commencement of the 12 month follow-up review; 20 recommendations were completed and had an ongoing aspect associated with their implementation; and, one recommendation was underway. The latter related to the implementation of the 12 month follow-up review, which can now also be categorised as completed.

4.3 For PM&C, a number of operational documents/artefacts have been updated/produced and processes/procedures strengthened in response to the Smith Review. Similarly, both AGD and ASD have acted on those recommendations that fell within their areas of responsibility.

4.4 Five elements of the work undertaken in PM&C warrant a specific reference:

- a new PM&C Security Framework was released in late 2018. The framework incorporates recommendations from the Smith Review and revisions to the Protective

Security Policy Framework (PSPF). The Framework is based on a set of principles and clearly articulates how protective security is managed within PM&C;

- complementary to the introduction of the new Security Framework, there has been a distinct shift within the Security team, away from the traditional compliance model of security management, to an acknowledgement of the role of the team as an educative and enabling service. Considerable effort has been made to strengthen relationships between the team and divisions. Positive results have been achieved across PM&C;
- a focus on positioning people to understand and actively model positive protective security behaviours has led to the introduction of a range of tools to educate and inform staff, including practical tip sheets, communications campaigns and re-designed training material;
- for the first time, an Instrument of Delegation (IoD) for all decisions relating to protective security is in place. The IoD outlines, in a clear and consistent way, the level of decision making required;
- capital funds were invested for the development of a new, fit-for-purpose protective security database. The database sources personnel information directly from Aurion, the Department's human resources and payroll system, as the 'single source of truth'. This enables the Security team to generate reports detailing trend analysis on protective security matters across divisions and branches. This tool is used to report protective security behaviours and practices to the Executive Board.

4.5 The focused work undertaken in PM&C, AGD and ASD since March 2018 on the implementation of the Smith Review recommendations has been significant. Progress on implementing the 28 recommendations has been highly satisfactory. However, judging the success of the implementation of the Smith Review recommendations requires a deeper analysis than simply ticking off against a 'traffic light' checklist. A qualitative assessment of the effectiveness and impact or otherwise of the recommendations is difficult. There are, however, a number of indicators which give confidence that the implementation of the Smith Review recommendations, led by PM&C, has been taken seriously across the APS and that the impact has been positive. Regardless, risk continues to exist as does the possibility of a future breach in the handling, storage and protection of sensitive and privileged information.

5. DEPARTMENT OF THE PRIME MINISTER AND CABINET

5.1 Several themes arose consistently across the focus groups I conducted:

- very positive views of the leadership response by the Secretary and the way he quickly and comprehensively responded to the initial breach;
- recognition that PM&C cannot allow a similar event to occur because of, both, reputational damage and a loss of confidence and trust in the Department by the Government and the wider APS;
- high level of awareness of the work undertaken since the Smith Review to strengthen process, procedures and training;
- the Department's Security team is now viewed as forward thinking and accessible rather than reactive and being behind closed doors;
- there is a greater level of conversation around the Department about the need to be security conscious in the handling, storage and use of sensitive and privileged information;
- staff at all levels expressed a willingness to 'call out' colleagues who exhibit poor security practices and assist those who may be ignorant of security requirements; this was generally described as 'looking out for each other' and protecting the Department.

5.2 The staff survey conducted in August 2018 showed that staff generally reported very strong security values. This included a belief that security is important and that security breaches pose significant risk to the Government, the Department and the public.

The survey also identified that teams who frequently and actively discuss security demonstrated a greater knowledge of security policies and protocols.

5.3 These are all positive indicators that a stronger security culture has been embraced by the staff of PM&C since the events of January 2018. The metrics available to SBS Branch tend to support this. For example, in June 2018 the Security team initiated a program of regular, after hours inspections of work areas to monitor compliance with the Department's clear desk policy. The overall trend in the ensuing 12 months has shown a steady decline in the number of breaches. A year-on-year comparison of statistics for June 2018 and May 2019 shows a drop of almost 50% in the number of breaches issued in the corresponding inspections in those months. Furthermore, zero breaches were reported for the inspections conducted during June 2019. The challenge for the Department is to ensure that this trend is maintained.

5.4 It is, however, only about 18 months since the ABC's *Cabinet Files* report and the consequential fallout from that event. It is my view that the continuing positive staff attitude toward, and focus on, security issues is still being driven by the lingering impact on the individuals caught up in those events and, more broadly, the likely sense of embarrassment and humiliation felt by all the staff in the Department as the good name, reputation and professionalism of the organisation was publicly disparaged. These are feelings common among staff in organisations that have suffered a negative seismic event that has been played out publicly. It does not take long, however, for these feelings and memory of the event to dissipate as staff with a direct understanding and recollection of the event and its consequences move on.

5.5 I was advised that PM&C has a high staff turnover rate, in the order of 23 to 25 percent per year. At this rate, the widespread populating of the Department by staff who were not affected by and have no direct recollection of the events of January 2018 will be rapid. As this occurs the focus on, and enthusiasm for, maintaining vigilance in relation to the proper handling, storage and protection of sensitive and privileged information will begin to diminish.

Measures that may have been put in place as a reaction to the events of January 2018, which can appear onerous for those who have no context, will in all likelihood be questioned, challenged or potentially ignored over time. This will most likely occur in the context of the quest for efficiency of process and/or dealing with workload pressures.

5.6 In terms of the priority and importance accorded to the proper handling, storage and protection of sensitive and privileged information, there was one noticeable difference in the focus groups between staff who were in the Department in January 2018 and those who arrived after the Smith Review. For those in the Department in January 2018 the need to focus on security came across as an innate and genuine desire to do the right thing and not repeat past mistakes. For those who had arrived after the Smith Review, 'security' was accepted as being important but was viewed more a rote process that had been articulated during departmental induction. There is a difference between doing something because you want to and because you are told you have to. I am not disparaging the professionalism and commitment of recent recruits but I do want to highlight a risk that needs to be addressed on an ongoing basis.

Finding 1: Protective security is a leadership issue

5.7 The SES-led communication campaign launched by the Secretary in early 2018 on security procedures and the handling of sensitive and privileged information cannot have a beginning and end date with a 'mission accomplished' exclamation at the end of it. On an ongoing basis the entire leadership team of PM&C must project in its messaging to staff, at every appropriate opportunity, the importance of maintaining a robust security regime. This messaging must come from all levels: Executive, Group, Division, Branch and Section. If the message is repeated often enough and seen to be a priority then it will be accepted as a priority. It will become an essential part of the fabric of the Department and an intrinsic element of being an officer in PM&C.

5.8 **Recommendation 1**: *It is recommended that the Executive Board commissions, endorses and rolls out a structured, long term, consistent communication strategy to be deployed at all leadership levels. The strategy should reinforce the importance of a robust departmental protective security environment and the role of individual staff in maintaining that environment. This element could form part of performance assessment discussions*.

5.9 Finding 2: Senior leadership must be aware of staff attitudes to protective security

5.10 The senior leadership of the Department must have, at any given time, a contemporary understanding of staff attitudes to protective security. Formal, periodic staff surveys are a critical tool in this context. To be useful the surveys must produce metrics that will give the leadership team a sound understanding of staff attitudes and, consequently, a lead on what remedial measures (if any) need to be put in place.

5.11 **Recommendation 2**: *It is recommended that regular staff surveys include questions which gauge staff attitudes to protective security; the findings from those surveys should be used to address any apparent waning in staff commitment to the maintenance of a robust security environment*.

5.12 Finding 3: Senior leadership must understand what the metrics are saying

5.13 It is critical that the Executive Board is assured that PM&C maintains an ongoing commitment to strengthening its protective security practices and culture. The Chief Operating Officer's monthly report and deep dive program would be an effective mechanism to provide this assurance. The deep dive program could be used to forensically examine protective security practices and behavioural trends. Protective security should be included in the deep dive program cycle, ideally no less than on a six monthly basis; perhaps even quarterly. Inclusion in the deep dive program has the additional advantage of oversight by the Operations Committee, thus ensuring an additional layer of assurance.

5.14 **Recommendation 3**: *It is recommended that 'protective security' be included in the Department's deep dive program reporting cycle, ideally no less than every six months.*

5.15 Finding 4: Standing up of taskforces in PM&C can create a risk to protective security

5.16 A further staffing-related risk which was raised with me relates to the practice of standing up subject matter specific taskforces in PM&C. These taskforces are usually time-limited and intense and involve bringing in to PM&C subject matter experts from other agencies. I was advised that the majority of staff who are seconded to these taskforces come from agencies that operate outside the general security, intelligence and law enforcement environment. Consequently, they can lack appropriate clearances and can, more broadly, be inexperienced in operating in an environment that has access to sensitive and privileged information, and where protective security is critical to daily operations. Consideration may

need to be given to limitations being placed on these staff which restricts their access to departmental systems that could be a pathway to sensitive and privileged information.

Any limitations would need to be constructed in such a way as to not be an impediment to these taskforces doing their job.

5.17 It is my view, however, that it is inevitable that any restrictions on systems access for seconded staff will create impediments for these taskforces. In that case, thought needs to be given to how to best prepare non-departmental staff to work in PM&C without generating risk that sensitive and privileged information is compromised, inadvertently or otherwise.

5.18 **Recommendation 4**: *It is recommended that consideration be given to developing an operational framework for seconding APS staff into PM&C which does not impede the prompt standing up of taskforces but which protects sensitive and privileged information holdings from unauthorised access by non-departmental staff.*

5.19 **Finding 5: Cabinet Division is building a robust protective security framework around Cabinet documents**

5.20 The Smith Review did not make any specific recommendations in relation to the work of Cabinet Division. It did acknowledge (paragraph 3.11 page 27 and Box 3, page 28) the work being done in the division to transform the way Cabinet documents are generated, distributed and stored. The implementation of the transformation program pre-dates the Smith Review and the *Cabinet Files* incident. I endorse the assessment of the Smith Review on the breadth and comprehensiveness of the transformation program being run by Cabinet Division and acknowledge that the work has continued apace in the period since the Smith Review.

5.21 Going 'paperless' through the digitisation of Cabinet documents, limiting access to that material and having a digital record of who accesses the material has and will enhance the protection of those documents. However, the risk identified by the Smith Review will continue. That is, it will not prevent officers across the APS who do have access to Cabinet and related material from creating and storing working documents outside the CabNet+ system. This risk is being mitigated through the ongoing training of staff across the APS who are responsible for the handling and management of Cabinet material. The Cabinet Liaison Officer (CLO) network is also being actively engaged to instil an appropriate security culture around Cabinet material within their home organisations. This training and engagement must be ongoing as all departments, as with PM&C, experience staff turnover.

5.22 The CabNet + Improvement Program has an explicit monthly reporting function where each participating Department and Agency is advised of the number of documents distributed to, and accessed by, users including unusual patterns of access. The full system is projected to be rolled out by the end of 2019.

Once the full system is rolled out, standard reports on usage will be available as a routine function which can be accessed by each participating agency.

5.23 **Recommendation 5**: *Cabinet Division should ensure that a combination of preventive and audit measures continue to be implemented across the APS to maintain a focus on the culture of protecting Cabinet documents. Findings from the audit measures should systematically be brought to the attention of the Executive Board and, as necessary, matters of concern referred to the Secretaries Board.*

6. ATTORNEY GENERAL'S DEPARTMENT

6.1 Recommendations 24, 25, 27 and 28 in the Smith Review were relevant to the Attorney-General's Department (AGD). The AGD advised that all four recommendations have been actioned and are described as 'Complete and Ongoing'. The AGD advised that benefits of implementation are already visible; for example, the establishment of the Chief Security Officer (CSO) Forum and a standing item on the Secretaries Board for updates on the Protective Security Policy Framework (PSPF) and reporting on security incidents.

6.2 CSOs in the wider APS characteristically carry multiple responsibilities within their organisations beyond their CSO role and, in many cases, would not have professional experience in the protective security context. These officers need and will benefit significantly from the AGD's support and outreach.

7. AUSTRALIAN SIGNALS DIRECTORATE

7.1 Recommendation 26 in the Smith Review addressed the work of the Australian Signals Directorate (ASD). The ASD advised that it has a number of initiatives under way that respond to and support Recommendation 26. The ASD's Australian Cyber Security Centre (ACSC) is establishing an APS-wide Chief Information Officer (CIO)/Chief Information Security Officer (CISO) forum to engage on cyber security issues. The forum is intended to be run monthly and commenced in June 2019. The forum will be used by ASD/ACSC to share sensitive, tailored threat information and cyber security risk advice, up to the 'Secret' level. Further, ASD advised that through the ACSC it is establishing a new internet presence, *cyber.gov.au*. This presence will give ASD the ability to share threat/risk information in a timely manner which will support agencies to enhance their cyber security.

7.2 The success and impact of the CIO/CISO Forum will be determined by the priority accorded to attendance by the CIOs and CISOs.

7.3 The ACSC has also begun to enhance its 'blue team' capabilities in support of its incident response and intelligence/threat capability. Blue teams comprise highly skilled cyber security specialists who can work with agencies to increase their cyber security posture. These teams will provide general and tailored advice as well as working closely with agencies to assist them to establish sound security architecture and cyber risk management processes.

8. THE WIDER APS

8.1 **Finding 6: CSOs in the wider APS need and welcome the assistance of AGD and ASD to help them meet their security obligations.**

8.2 As noted in paragraph 3.6, I met with officers with responsibility for protective security from various APS agencies. My objective was to try and ascertain the extent to which the consequences of the *Cabinet Files* incident and the recommendations of the Smith Review impacted on these agencies. These agencies were chosen as they are of a significant size and they generally operate outside the intelligence, security and law enforcement sphere, in an environment where protective security may not be front-of-mind. While my sample space is small, the views expressed were consistent and do raise some issues of concern.

8.3 Common themes that were brought to attention included:

- there was immediate action after the ABC's report to undertake an immediate audit of all security containers and their contents;
- there was quick action by Secretaries to appoint CSOs after the Smith Review in order for their departments to be compliant with the push from PM&C for greater focus on protective security;

- some staff appointed to the CSO positions carried much wider responsibilities in their departments, some of which had a higher priority than protective security within the context of each department's immediate operations and pressing priorities;
- the extent to which each CSO is equipped to meet the associated set of responsibilities was essentially driven by her/his level of enthusiasm and her/his initiative to identify what tools, skills and training were required and what protective security strategies needed to be put in place;
- there was acknowledgement that both ADG and ASD had activities in train which will assist the CSOs to meet their obligations but greater priority, assistance and coordination across the APS was desired if a consistent approach is to be achieved. The CIO/CISO Forum run by ASD in June 2019 was a welcome initiative.

8.4 The advice provided by both AGD and ASD indicates that CSOs will get the support and guidance they need but it is early days.

8.5 **Recommendation 6**: *Agencies which operate outside the general security, intelligence and law enforcement environment to be comprehensively engaged to determine: if their protective security capability meets the requirements for a consistent and robust whole-of-APS approach to protective security; if their need for external assistance is being met; if protective security gaps exist; and what further action is required to strengthen whole-of-APS capability and consistency of approach to protective security.*

8.6 **Finding 7: Smaller, specialty agencies attached to Departments play a key role in the protective security agenda and need to be equally as rigorous in their efforts.**

8.7 It will be critical to ensure the smaller 'satellite' agencies are engaged in the broader protective security agenda, and can similarly call on ASD and AGD for assistance in meeting their obligations. From a preventative perspective, given many of these smaller agencies operate on IT systems linked to the parent department, it is crucial they too have robust systems to ensure overall stability and reduce the risk of penetration to government information. Pleasingly, CSOs in the satellite agencies expressed an eagerness to be involved in this whole-of-government effort.

8.8 Taking a deeper dive into the interconnectivity of Commonwealth systems and their vulnerabilities was beyond the scope and technical competence of my review. The ASD's ACSC, however, appears to be an appropriate vehicle to undertake this task given its existing APS engagement through the CIO/CISO forum.

8.9 **Recommendation 7**: *A detailed, whole-of-APS assessment be undertaken of the protective security environment, to include agencies attached to Commonwealth departments,*

9. LESSONS FOR ALL

9.1 My engagement with Home Affairs confirmed that even for an agency that does operate in the security, intelligence and law enforcement environment there were lessons and benefits from the Smith Review and associated recommendations. Home Affairs has a well-resourced, robust protective security framework and an associated assurance framework. The *Cabinet Files* incident and findings and recommendations of the Smith Review did, however, provide the impetus to progress a number of matters. For example: a new Agency Security Plan, framed in accordance with the revised PSPF, has been signed off by the Secretary; the office of the CSO in partnership with the Facilities and Records Management area reviewed and upgraded processes and procedures for monitoring the chain of possession of security containers and their contents; prescribed monitoring, reporting and escalation procedures have been implemented to manage security breaches.

The assurance methodology associated with these activities is producing the data required to understand staff behaviour and identify any trends that may require remedial action.

9.2 As with other agencies, Home Affairs does, however, face the ongoing challenge of maintaining staff focus on and commitment to protective security. This is particularly challenging for a large and complex agency which covers the broad spectrum of social policy, economic policy, security, intelligence and law enforcement. Home Affairs addresses this challenge by maintaining a high visibility posture on protective security. The Department does this though appropriate on-boarding procedures for new staff and ongoing mandatory training on security and related issues. Most importantly, however, there is regular and consistent messaging from the leadership group to all staff on the importance of maintaining protective security.

Summary of Recommendations

Recommendation 1: It is recommended that the Executive Board commissions, endorses and rolls out a structured, long term, consistent communication strategy to be deployed at all leadership levels. The strategy should reinforce the importance of a robust departmental protective security environment and the role of individual staff in maintaining that environment. This element could form part of performance assessment discussions.

Recommendation 2: It is recommended that regular staff surveys include questions which gauge staff attitudes to protective security; the findings from those surveys should be used to address any apparent waning in staff commitment to the maintenance of a robust security environment.

Recommendation 3: It is recommended that 'protective security' be included in the department's deep dive program reporting cycle, ideally no less than every six months

Recommendation 4: It is recommended that consideration be given to developing an operational framework for seconding APS staff into PM&C which does not impede the prompt standing up of taskforces but which protects sensitive and privileged information holdings from unauthorised access by non-departmental staff.

Recommendation 5: Cabinet Division should ensure that a combination of preventive and audit measures continue to be implemented across the APS to maintain a focus on the culture of protecting Cabinet documents. Findings from the audit measures should systematically be brought to the attention of the Executive Board and, as necessary, matters of concern referred to the Secretaries Board.

Recommendation 6: Agencies which operate outside the general security, intelligence and law enforcement environment to be comprehensively engaged to determine: if their protective security capability meets the requirements for a consistent and robust whole-of-APS approach to protective security; if their need for external assistance is being met; if protective security gaps exist; and what further action is required to strengthen whole-of-APS capability and consistency of approach to protective security.

Recommendation 7: A detailed, whole-of-APS assessment be undertaken of the protective security environment, to include agencies attached to Commonwealth departments,

ATTACHMENTS:

Attachment 1: Smith Review Terms of Reference

Attachment 2: Terms of Reference for the 12 month follow-up review

TERMS OF REFERENCE

Review of the Department of the Prime Minister and Cabinet's security procedures, practices and culture

February 2018

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 safeguards 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 safeguarding 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.

TERMS OF REFERENCE

Implementation of the 'Smith Review' and progress in strengthening protective security procedures, practices and culture: 12 month follow-up review

March 2019

INTRODUCTION

On 23 March 2018, Mr Ric Smith AO PSM delivered an independent review of the Department of the Prime Minister and Cabinet's (PM&C's) security procedures, practices and culture, including the implications for the Australian Public Service more broadly.

All recommendations were agreed in full, with the 'Smith Review' published to ensure the widest possible awareness of its findings across the Australian Public Service (APS).

The Review was commissioned by the Secretary of PM&C in response to the loss of classified Commonwealth material, leading to the ABC's publication of a range of Cabinet documents on a webpage, "The Cabinet Files", on 31 January 2018.

The 'Smith Review' concluded that PM&C should strengthen the high-level governance of its protective security responsibilities, and demand a more robust security culture in the organisation. The 'Smith Review' considered the environment in which protective security must be managed within PM&C and made 28 recommendations about:

- the protective security governance arrangements in place in PM&C;
- the existing documentation in PM&C, including practices, systems and procedures relating to protective security;
- PM&C's culture in regard to protective security and its relevant training programs; and
- Implications for the broader APS, including lessons that might be drawn from the Review for other agencies.

This included a recommendation that a further review be undertaken after 12 months to confirm that agreed recommendations have been implemented and, to the extent possible, to measure their effectiveness.

PURPOSE AND SCOPE

This review will consider progress to date in strengthening PM&C's protective security procedures, practices and culture protective security culture. It will also include recommendations to guide ongoing efforts to mature protective security culture across the Department and broader APS. This will include a focus on:

- the extent to which 'Smith Review' recommendations have been implemented and, to the extent possible, the effectiveness of these recommendations;

- broader activities undertaken to strengthen protective security culture across PM&C and the APS; and

- progress in strengthening PM&C's formal and informal security culture, informed by an analysis of data for which baselines are available.

TIMING

A Preliminary Report will be delivered to PM&C's Deputy Secretary Governance as soon as practicable. It is envisaged that a Final Report be provided by 31 May 2019.