14 May 2019

Review of the Department of Veterans' Affairs security and investigations functions

Philip Moss AM

Independent Reviewer

Mr Mark Cormack
Deputy Secretary
Department of Veterans' Affairs
Canberra ACT

Dear Mr Cormack

I am pleased to give you my final report of the review I have conducted into the Department's security and investigations functions. The review commenced on 29 October 2018.

The report has been completed in the light of the response to the draft report, which was provided on 3 March 2019 for the purposes of procedural fairness and accuracy.

The terms of reference required the review to consider also the Department's Unreasonable Complainant Conduct Framework (UCCF) and the role of the Client Liaison Unit (now known as the Managed Access unit). The UCCF and Managed Access are not directly related to the role of the security and investigations team. Accordingly, the review has two distinct focuses, which are dealt with separately.

I take this opportunity to acknowledge the willingness of staff members of the Department to assist the review and the support which Mr Simon Hill has provided.

Yours sincerely

s 47F

Philip Moss AM
Independent Reviewer

14 May 2019

Contents

Terms of Reference

A Review of the Department of Veterans' Affairs (DVA) security and investigations function is to be undertaken to assess its appropriateness for the environment within which the Department operates.

The Security and Investigations team currently has responsibility for personnel security; in partnership with the Client Engagement and Support Services Division and Veterans and Veterans Families Counselling Service,[1] the assessment of clients considered at risk of self-harm; investigations relating to fraud and other matters; physical security at DVA events; and advice relating to the handling of classified information.

The Department is operating in a complex and sensitive environment and as part of its Transformation journey, is reviewing its systems, processes, workforce and operating model. It is now timely to review the security and investigations function to ensure their ongoing alignment with the future direction of the Department and that it will provide the services required as the Department adjusts it workforce and operating model.

The review will consider:

- the processes for the handling of critical security incident responses and investigations;
- arrangements in place to ensure physical, personnel and information security (other than IT Security);
- the role of the security team in triaging and assessing veterans identified at risk;
- the role played by the security team in supporting DVA's national and overseas events, including commemorations;
- the appropriateness of the security and investigations team's resourcing, training, credentials and capability compared to APS agencies with a similar function;
- the implementation of the recommendations from the Review of the Department of the Prime Minister & Cabinet Security Procedures, Practices and Culture. In particular, DVA 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 appropriateness and effectiveness of the Department's Unreasonable Complainant Conduct framework and the role of the Client Liaison Unit ; and
- any other matters relating to the Department's security and investigations functions which the reviewer deems suitable and relevant to the review.

[1] Since 19 October 2018, this service has been known as Open Arms – Veterans and Families Counselling.

Executive Summary

Background

1.1 The background to this review of the Department's security and investigative functions is its Transformation journey, which is underway. The purpose of the Transformation journey is to refocus the Department's efforts to put veterans and their families first by adapting its operating mode, changing the way it delivers services and developing better communication. The review's purpose is to ensure that the Department's security and investigations functions capability is aligned with the Transformation journey.

1.2 The Department's Security and Investigations Section, as is the Department overall, is in a dynamic state. The Protective Security Policy Framework (PSPF) has been revised and needs to be implemented. The Productivity Commission is in the process of finalising its report entitled *A Better Way to support Veterans*, which suggests changed arrangements for the delivery of commemorative events. The review of the Department of the Prime Minister and Cabinet's security procedures, practices and culture has produced outcomes which are relevant to all Australian Public Service departments and agencies, including DVA.

Processes for Handling Critical Security Incidents

1.3 A critical security incident covers a wide range of events including "any incident where a staff member is in immediate fear for the safety or wellbeing of themselves, another staff member, a client and/or a member of the public" as well as loss, damage or theft of property, compromise of official information emergency incidents and unauthorised access.

1.4 The relevant document is the Managing Critical Security Incident Protocol (the Protocol). The Security team's processes in practice have evolved significantly from the Protocol. There is a need to review such documentation on a regular basis. See **Recommendation 1**.

1.5 There is a need to distinguish the responses to critical security incidents involving client risk of self-harm from other critical security incidents. Under the current protocol, any Department staff member can call 000 if there is an immediate risk of client self-harm. This procedure needs to be revised. See **Recommendation 2**.

1.6 Usually, the Security team is at the centre of the critical security incident response when there is imminent risk of client self-harm. The response in such circumstances is for the Security team to call 000. The conclusion is that the current approach of using the critical security incident framework, when there is imminent risk of client self-harm, is no longer suitable. See **Recommendations 3 & 4**.

1.7 Although the Protocol provides for client threat of self-harm to be referred to the Security team, which then may contact emergency services, other processes are also being used within the Department. For example, Open Arms – Veterans and Families Counselling has adopted the approach that only its senior clinicians contact emergency services.

1.8 Department staff members need to have an increased level of positive engagement with clients. The requirement is for them to understand the principles of trauma-informed service delivery and ways of relating to people who are difficult, not because such clients are trying to be difficult, but because they may be unwell. The requirement is also for staff training to include enhanced suicide awareness and mental health awareness. See **Recommendation 5**.

<u>Arrangements to ensure physical, personnel and Information Security (other than IT Security)</u>

1.9 The Security team is responsible for a range of documents relating to physical, personnel and information security. Recently, it has drafted the Department's response to the revised Physical Security Policy Framework (PSPF). The PSPF mandates the appointment of a Chief Security Officer and the establishment of a Security Governance Committee, which is pending.

1.10 Matters relating to complacency concerning classified material and a lack of a system to track the movement of safes in the Department were brought to the review's attention. The conclusion is that such matters reflect adversely not only on the Department's security practices, but also indicate that its security culture may need to be reset. The need for a similar focus on security training and behaviour is pressing. See **Recommendation 6**.

1.11 The Smith Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture makes it clear that the required emphasis in relation to security is on culture. Accordingly, the FAS Business Support Services position is the most suited to perform the role of Chief Security Officer. See **Recommendation 7**.

1.12 The review was told that a lack of discipline is evident concerning the distribution of Cabinet documents. The conclusion is that there must be explicit understanding about who is responsible in relation to handling such material and who is responsible. See **Recommendations 8 & 9**.

1.13 The review's terms of reference exclude consideration of IT security. However, the review was told that since information security was fundamentally connected to IT security, a further review of this aspect would be needed. It was suggested to the review that the Department would need to acquire the capacity to conduct investigations into IT security matters.

Role of the Security team in triaging and assessing veterans identified at risk

1.14 The Security team regards its role in relation to triaging and assessing clients at risk as evaluating whether the risk is immediate. If there is immediate risk, the Security team calls emergency services and informs the Triage and Connect team subsequently. If no immediate risk, the Security team passes the information it has gathered to Triage and Connect for it to undertake triage.

1.15 Open Arms policy concerning its response to clients at risk, namely that only senior clinicians contact emergency services and that decisions about responses are made by a clinical team, not an individual, should be adopted as the Department's new standard. Applying Open Arms' policy to the Triage and Connect process promises an enhancement of current arrangements.

1.16 Accordingly, the responsibility for all critical security incidents involving client threat of self-harm, including immediate risk, should be transferred from the Security team and become the function of Triage and Connect. See **Recommendation 10**.

1.17 The use of the term critical security incident when there is a risk of client self-harm is inappropriate and needs to change. See **Recommendation 11**.

1.18 The Department needs to develop the capacity to analyse critical incidents with the aim of understanding why they occurred and to take measures to prevent recurrence. See **Recommendation 12**.

1.19 The Department's lack of a single case management system is a recurring theme. There should be a central repository of holistic information regarding clients who are perceived to need additional support, for timely use if self-harm is threatened. See **Recommendation 13**.

Role of the Security team in supporting national and overseas events, including commemorations

1.20 The Department's purpose is to support those who serve or have served in the defence of Australia and commemorate their sacrifice. One of the ways that it fulfils this purpose is through commemorations.

1.21 The Department is involved with a broad range of commemorative events, both nationally and overseas and is the lead agency for annual commemorative events at Gallipoli and Villers-Bretonneux. As such, it is responsible for security arrangements.

s 33, s 47E

1.29 As to the Investigations team, which is dispersed with five officers in four different locations, statistics relating to fraud investigation indicate that its capability in relation to dealing with fraud allegations is limited. The need to drive outcomes seems to be lacking. No monies have been identified for recovery. A significant number of matters were carried over from the previous financial year to the present year.

1.30 Recruitment action is needed for both the Security and Investigations teams. In the case of the latter, the opportunity is available to augment the investigative skillset. Another option would be to outsource the fraud investigation function to another organisation, while a third option would be to make arrangements for an investigative partnership, when needed, with another agency. See **Recommendations 15, 16 & 17**.

1.31 The Security and Investigations Section occasionally supports Public Interest Disclosure (PID) investigations, which are coordinated in the People Services Branch. The PID Act and the Australian Public Service (APS) Code of Conduct are key elements of the Department's integrity framework, with particular reference to corrupt and fraudulent conduct.

1.32 During 2017-18, 14 PID investigations were completed of which ten resulted in possible disciplinary action. About 70% of these investigations related to personal employment-related grievances. It is noted that there have been no recent PID matters relating to fraud. In this context, the challenge is to invoke a Department-wide awareness and use of the integrity perspective of PID. See **Recommendation 18**.

1.33 The review consulted with the representatives of the Australian Taxation Office (ATO) and the Department of Human Services (DHS). Unlike DVA, the ATO is not in a care role for its clients. When an ATO client makes a threat of self-harm, the ATO response is to report the matter to the police. No other action is considered necessary. However, this approach is changing.

1.34 The digital environment is having a significant impact on ATO staff members. Sometimes incidents occur of on-line aggression, harassment and targeting that can cross over into private life. From time to time, ATO clients attempt to contact ATO staff members through personal channels.

1.35 A recently established (February 2019) Security Intelligence Unit (SIU) will meet the need in the ATO to have a centralised function for security and intelligence. At present, there is no centralised knowledge of risk, or point of contact for business areas, when dealing with complex clients. Business areas themselves do not have the necessary capability.

1.36 In DHS, the Child Support program is the source of most client threats of self-harm. The size of DHS, through the bringing together of three large programs (Centrelink, Child Support and Medicare), means that slightly different processes persist. Ultimately, client threats of self-harm are referred to the Physical Security and Operations Section and can end up with a call to 000 for an emergency services response. In that case, the procedure is for the officer who received the call to ring. However, in a prior step, DHS social workers are brought into the process, whenever possible.

1.37 Both the ATO and DHS are engaging with similar issues as the DVA, which could learn from their experience.

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

1.38 The Department's response to the Smith review has been minimal, although the Security team has focused on security culture in line with the Smith review recommendations through drafting the response to the revised Protective Security Policy Framework.

1.39 The Department needs to focus on the Smith review recommendations in a comprehensive and systemic way. This focus should come from the Security Governance Committee, when established, and the Security team. The claim that "we [have] done everything that was required of us, as an agency, as a result of the recommendations of the Smith review" is unwarranted.

1.40 The focus should be not only to implement the Smith review recommendations for the APS, but also, with the necessary changes being made, the recommendations relating to PM&C. See paragraph 3.9 of this report and **Recommendation 19**.

Appropriateness and effectiveness of the Department's Unreasonable Complainant Conduct Framework and the role of the Client Liaison Unit

1.41 The Unreasonable Client Conduct (UCC) Framework is administered by the Managed Access team, which is part of the Client Coordination and Support Branch. Previously called the Client Liaison Unit (CLU), Managed Access commenced in September 2018.

1.42 The CLU was established in 2007 for clients whose cases were complex because their relationship with the Department had become untenable, and/or significant behavioural issues were evident.

1.43 The UCC policy is based on the Ombudsman *Managing Unreasonable Complainant Conduct - Practice Manual*. The use of language in the UCC policy changes after the first few paragraphs from 'client' to 'complainant'.

1.44 The use of terminology is important. To refer to particular clients as complainants indicates transformation to a different status. Accordingly, it is an unfortunate label which has been applied to certain clients by adopting the Ombudsman practice manual without appropriate adaptation and modification.

1.45 The UCC Framework policy needs to be revised to remove any possible misunderstanding or doubt about the Department's commitment to assist all veterans (as clients) and their families. See **Recommendation 20**.

1.46 A view expressed to the review is that the UCC Framework is a very good mechanism, provided it is used sparingly.

s 47F

1.47 The approach which Managed Access adopts is to engage and build rapport with its clients. The intention is to try and resolve the matter relating to the cause of the referral under the UCC Framework.

1.48 Since October 2018, Managed Access has been developing an advisory role. The aim is to provide support to business areas interacting with clients who may be displaying unreasonable conduct. Since the implementation of the advice line program, the Managed Access team has been consulted on 10 cases, none of which has progressed to a referral to, or acceptance of, a client under the UCC Framework.

1.49 Managed Access staff members told the review of their observation when delivering training that there is a skill gap in client-facing staff members in business areas about how to converse with clients. Since Managed Access has published its advice line, it has seen an increase in requests for advice and a reduction in referrals. This result is attributed to staff members contacting Managed Access earlier and managing behaviour within their business areas more than previously.

1.50 The Managed Access team is achieving best practice. It is achieving this outcome by restoring the relationship with a number of UCC Framework clients, through systemically reviewing the need for clients to enter, and remain under, the UCC Framework and supporting and advising Department client-facing staff members about dealing with unreasonable client conduct in order to reduce the incidence of referral to the UCC Framework. See **Recommendations 21, 22 & 23**.

1.51 The Managed Access approach could be expanded and applied more broadly. In order to restore the relationship with clients under the UCC Framework, and other clients who are disaffected, an approach needs to be considered which would be proactive and draw the line on past negative experience, some of which may have its origin prior to contact with DVA. Such an approach would involve a framework in which there is a commitment to understand the client experience and to respond in a meaningful way so as to bring closure for the client. The idea has been described to the review as a restorative justice approach, but it could also involve the use of conciliation. See **Recommendation 24**.

1.52 The Department needs to develop a concentrated focus on providing its client-facing staff members with the skills and training needed to achieve optimal outcomes. See **Recommendation 25**.

1.53 The Productivity Commission Draft Report notes that the need for policy which anticipates crises before they occur and making changes in the long term interest of veterans instead of policy change that is reactive. Some client-facing Branches have the potential for greater incidence of unreasonable client contact. The Department needs become more predictive by developing the capacity to identify in a comprehensive and systematic manner the indicators which result in client escalation. See **Recommendation 26**.

Summary of Recommendations

This summary lists each recommendation under the relevant criterion of the terms of reference.

Criterion 1. The process for the handling of critical security incidents responses and investigations.

Recommendation 1: That the *Managing Critical Incident Protocol* (or its replacement) be reviewed on a regular basis, at least annually.

Recommendation 2: That Department staff members be required in the first instance to report all critical security incidents involving client threat of self-harm to the Department's nominated point of contact.

Recommendation 3: That the Department's current processes for engaging clients who threaten self-harm are no longer appropriate and that revised processes be developed based on a clinical framework and the involvement of clinicians.

Recommendation 4: That the Department develop partnerships with State and Territory mental health services as part of revised processes for engaging with clients who threaten self-harm.

Recommendation 5. That Department review and revise its current suicide awareness and mental health awareness so that client-facing staff members are provided annually with face-to-face training.

Criterion 2. Arrangements in place to ensure physical, personnel and information security (other than IT Security).

Recommendation 6: That the Department adopt the relevant recommendations of the Smith Review (of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture) in relation to security culture, training and behaviours, namely

- **the Secretary and Deputy Secretaries should lead in raising awareness and accountabilities for security**
- **All Canberra-based new starter staff members should be required to undertake face-to-face security training within the first week of commencing at DVA** (The Department has advised that this requirement is being met.)
- **All regional new starter staff members should be required to complete mandatory online training within a week of commencement** (The Department has advised that this requirement is being met.)

- **The effectiveness of the Department's security training should be evaluated regularly**

- **Random internal security checks and periodic independent audits of staff security and the storage of classified information should be undertaken.**

Recommendation 7: That the FAS Business Support Services be appointed as the Department's Chief Security Officer.

Recommendation 8: That the Secretary issue a delegation or direction to the Assistant Secretary Parliamentary and Executive Support to be responsible for all aspects relating to the handling of Cabinet documents, including security policy.

Recommendation 9: That, noting the recommendations of the Smith Review, the Department develop a training and information package to increase awareness and understanding among its staff members about Cabinet document handling and storage.

Criterion 3. The role played by the Security team in triaging and assessing veterans identified at risk.

Recommendation 10: That all incidents of client threat of self-harm be referred to the Triage and Connect team instead of the Security team.

Recommendation 11: That the term 'critical security incident', when applied to client threat of self-harm, be replaced by different terminology which indicates the Department will provide whatever support necessary to a client.

Recommendation 12: That the Department develop the capability, not only to respond to critical incidents, but also to analyse them in order to improve understanding of why they have occurred.

Recommendation 13: That, in the context of client threat of self-harm or harm to others, the Department develop the capability to provide holistic information about its clients in a timely manner.

s 33, s 47E

Criterion 5. The appropriateness of the security and investigations team's resourcing, training, credentials and capability compared to APS agencies with a similar function.

Recommendation 15: That recruitment action be taken to increase the Security team by one full-time equivalent APS 6 position and to bring both the Security team and the Investigations team to their full-time equivalent staffing levels.

Recommendation 16: That the Investigations team establish contact with the Commonwealth Director of Public Prosecutions to ensure that briefs of evidence are prepared with the optimal chance of prosecutorial success.

Recommendation 17: That consideration be given to outsourcing the Department's fraud investigation function or entering an investigative partnership arrangement with another department or agency.

Recommendation 18: That the Department's capability to use the Public Interest Disclosure Act framework and handle PID Act matters effectively be ensured.

Criterion 6. The implementation of the recommendations made in the report of the Review of the Department of the Prime Minister & Cabinet Security Procedures, Practices and Culture. In particular, DVA 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.

Recommendation 19: That the Department give priority to implementing the recommendations of the Smith review and engage in a systematic and comprehensive response to it with a view to integrating those recommendations into its own security procedures, practices and culture.

Criterion 7. Consider the appropriateness and effectiveness of the Department's Unreasonable Complainant Conduct (UCC) framework and the role of the Client Liaison Unit.

Recommendation 20: That the Unreasonable Complainant Conduct Framework policy be revised to remove any possible misunderstanding or doubt about the Department's commitment to assist all its clients and their families.

Recommendation 21. That the Department continue to reduce the number of clients under the Unreasonable Client Conduct Framework.

Recommendation 22: That the Managed Access advisory service be developed further as a resource to assist and support the Department's client-facing staff members.

Recommendation 23: That the UCC Framework be comprehensively revised, including its nomenclature, to reflect current Managed Access practice.

Recommendation 24: That the Department aim to restore the relationship with disaffected clients, both under the UCC Framework and beyond, by establishing a program which is committed to developing understanding of the client's past negative experience, developing trust and providing such a response as to bring closure for the client.

Recommendation 25: That the Department develop a concentrated focus on providing its client-facing staff members with the skills and training needed to achieve optimal outcomes for clients.

Recommendation 26: That the Department develop the capacity to identify in a comprehensive and systematic manner the indicators which result in client escalation.

Conduct of the Review

1.1 In conducting the review, the review team spoke with a wide range of the Department's staff members. The review spoke also with representatives of the Department of Human Services and the Australian Taxation Office.

1.2 The review obtained and read documents relevant to the terms of reference, including the Draft Report of the Productivity Commission entitled *A Better Way to Support Veterans*, which was released publicly on 14 December 2018.

1.3 The review gave particular attention to the processes for handling critical security incidents and the role played by the Security team in triaging and assessing veterans at risk. In the context of the Department's Transformation journey, with its focus of putting veterans and their families first, these aspects of the terms of reference assumed a particular importance.

1.4 During the course of the review, additional matters relevant to the terms of reference were brought to the review's attention. For example, specific incidents occurred about an aspect of the operation in the Department of the *Public Interest Disclosure Act 2013* and the process of keeping track of secure cabinets. The review was briefed about those matters and they were taken into account.

The Review

Background

The background provides detail on the undertaking of the Review. It also describes the environment in which the Department operates and why this review has been conducted.

The environment in which the Department operates

1.1 The environment in which the Department operates is changing. In its submission to the Productivity Commission Inquiry into Compensation and Rehabilitation for Veterans, the Department noted that:

> *DVA has recognised that its services, approaches, processes and culture have not always kept pace with the changing needs and expectations of its veteran clients; nor has DVA kept up with community standards for service delivery, accessibility or engagement. DVA has listened to feedback from the veterans' community indicating that improvements are required.*[2]

1.2 The Department is undergoing transformation. It has additional Government funding for that purpose. In its 2017-18 Annual Report, it is stated that this transformation, now in its second year and referred to as the Transformation journey or Transformation program,[3] is to ensure that the Department is better able to serve veterans and their families. One challenge, said to be the greatest, is to rebuild trust between the Department and former and serving Australian Defence Force (ADF) personnel and their families.[4]

1.3 This transformation journey is said to be "driven on a top down basis", with the Secretary closely involved in the broad direction of veteran-focussed design and service delivery.[5] It seems that the Department is in a 'two-speed' phase. At the executive level, there is alignment with the new direction, which is in the process of reaching down to the Department as a whole.

[2] Department of Veterans' Affairs, Submission to the Productivity Commission Inquiry into Compensation and Rehabilitation for Veterans, July 2019, p. v.
[3] It is also referred to as the Veteran Centric Reform Program.
[4] Department of Veterans' Affairs, *Annual Report 2017-18*, pp. 3 & 5.
[5] Interview, p. 5.

1.4 Through this transformation, the Department is adapting its operating mode, changing the way it delivers services and working out better ways to communicate about what it does.[6] The Annual Report also notes that, after 100 years of repatriation, the Department is refocusing its efforts to put veterans and their families first, delivering the services they need where and when they need them, restoring confidence that the wellbeing of veterans and their families is the Department's prime focus.[7]

1.5 Comments about the environment in which the Department operates have been made in two significant reports. The first is the Senate Foreign Affairs, Defence and Trade References Committee Inquiry report, entitled *The Constant Battle: Suicide by Veterans*. In that report, it is noted that the unique feature of that Inquiry was to examine the framework of military compensation arrangements and its administration through the lens of suicide by veterans.[8]

1.6 The Inquiry report cited an Australian Institute of Health and Welfare summary report released in June 2017 that stated,

> *[t]he suicide rates of ex-serving men were more than twice as high for those serving full-time or in the reserve.*
>
> *ex-serving men aged 18-24 were at particular risk – 2 times more likely to die from suicide than Australian men of the same age.*[9]

1.7 In response to the Inquiry report, the Australian Government stated that it would continue to develop and implement specific suicide prevention programs targeted at those veterans identified in at-risk groups.

1.8 Another aspect of the Department's operating environment is the Department's future operating model. Under business cases developed as part of the Veteran Centric Reform Program, one possibility is that the Department could outsource various service delivery functions to other government agencies, for example to the Department of Human Services. An exception would be complex cases which the Department would retain. In that context, the capability to relate effectively to clients with complex cases would continue to be fundamentally important.

1.9 The second significant report appeared in December 2018 when the Productivity Commission released a draft version of *A Better Way to Support Veterans.* This report notes that:

---

[6] *DVA Annual Report 2017-18*, p. 6.
[7] DVA Annual Report 2017-18, p. 6.
[8] The Senate, Foreign Affairs, Defence and Trade References Committee, *The Constant Battle: Suicide by Veterans*, August 2017, p. xvii.
[9] The Senate, Foreign Affairs, Defence and Trade References Committee, *The Constant Battle: Suicide by Veterans*, August 2017, p. 16.

[T]he environment in which the system is operating has changed. The nature and tenure of military service has changed, as have approaches to social insurance and the availability of mainstream health and community services. The community of Australian veterans and their families is also changing and the new generation of veterans have different needs and expectations.[10]

1.10 As stated in the Productivity Commission's draft report, the message is that the current veterans' compensation and rehabilitation system is not 'fit for purpose' – it requires fundamental reform.[11]

Why is this review being conducted now?

1.11 As stated in the review's terms of reference, the Department is operating in a complex and sensitive environment and, as part of its Transformation journey, is reviewing its systems, processes, workforce and operating model.

1.12 One comment made to the review is that Department staff members need to be able to access advice when client issues escalate. There is said to be a vacuum which the security team is currently filling.

1.13 The Department is in a dynamic state. For example, the Triage and Connect team has been established and is developing its processes, an internal audit of the Unreasonable Client Conduct Framework (UCC framework) and Client Liaison Unit (CLU) (now known as Managed Access) has been finalised, and an organisational structure occurred in mid-2018 and was subsequently fine-tuned in December.

1.14 The present review of the Department's security and investigations functions is part of the Transformation journey. The Department is seeking a more integrated engagement with its clients. Clients are being engaged more closely. Hence, it is important that the Department has the right security framework and processes in place.[12] The review's purpose is to ensure that these functions are aligned with the future direction of the Department and that the Security team and Investigations team provide the services required as the Department adjusts its workforce and operating model.[13]

[10] Productivity Commission, Draft Report December 2018, *A Better Way to Support Veterans*, p. 4.
[11] Productivity Commission, Draft Report December 2018, *A Better Way to Support Veterans*, p. 4.
[12] Interview, p. 1.
[13] See the review's terms of reference.

1.15 As to the Department's UCC framework and the Client Liaison Unit (now known as Managed Access), there has been concern that the referral of some clients under the UCC framework has contributed to the breakdown in the relationship between veterans and the Department. A different approach is being adopted. It is one of engagement led by the Secretary and the Executive. Hence, the need exists to consider the appropriateness and effectiveness of the UCC and the Managed Access team.

1.16 During 2018-19, the Government initiated two reviews into the delivery of services and support for veterans and their families.[14]

Protective Security Policy Framework

1.17 The Protective Security Policy Framework (PSPF), which is promulgated by the Attorney-General's Department, is the framework to assist Australian Government entities to protect their staff members, information and assets. It outlines roles and responsibilities that align with the *Public Governance, Performance and Accountability Act 2013* (the PGPA Act).

1.18 All Australian Public Service departments and agencies must meet the PSPF requirements, implement effective responsibility and reporting structures and promote a positive security culture.

1.19 An updated PSPF[15] has been issued and was received by the Department in October 2018. Compliance with the new framework is due by August 2019.

[14] The Productivity Commission is reviewing the compensation and rehabilitation system of support, while a scoping study has been undertaken into the Veterans' Advocacy and Support Services.
[15] PSPF (2018).

Chapter 1 – Consider the processes for the handling of critical security incident responses and investigations

This chapter outlines the processes for the handling of critical security incidents and investigations relating to fraud and public interest disclosure.

Critical Security Incidents

What is a critical security incident?

2.1 The relevant Department document is the *Managing Critical Incident Protocol* (the Protocol).

2.2 The Protocol states that "a critical security incident includes any incident where a staff member is in immediate fear for the safety or wellbeing of themselves, another staff member, a client, and/or a member of the public". The examples given include: "instances of harm to oneself or others; a direct threat of harm to oneself or others; and violent, antisocial and/or aggressive behaviour".[16]

2.3 According to the Protocol, critical security incidents "can also include: assault; threatening, abusive or offensive behaviour; threat of self-harm; loss, damage or theft of property; compromise of official information; damage to DVA or a contractor's physical environment; emergency incidents (such as bomb or chemical threats); attack on the ICT environment; and trespass or unauthorised access".[17]

2.4 It is noted that the term 'critical security incident' covers a broad range of events.

Documentation relating to critical security incidents

2.5 The Protocol is undated and unsigned. It appears to have been amended most recently in September 2018. The Security and Investigations Section is responsible for the Protocol.

2.6 The purpose of the Protocol is "to standardise the assessment and response from [the] DVA Security team member managing a critical incident". It provides guidance by outlining the actions the Security team is to take during a critical security incident and the process for assessment and reporting.[18]

[16] Department of Veterans' Affairs, *Critical Security Incident Protocol*, p. 5.
[17] Department of Veterans' Affairs, *Critical Security Incident Protocol*, p. 5.
[18] *Managing Critical Security Incident Protocol*, p. 3.

2.7 The Protocol states that the Security team is responsible for protecting critical assets – people, property, information and reputation and address-related incidents in accordance with the PSPF.[19] [20]

2.8 It is noted that the Protocol distinguishes between different types of critical security incidents, but that it does not provide for different processes. Instead, it refers interchangeably to a broad range of events, but which are all based on the same response framework.[21]

2.9 It is also noted that the Protocol identifies a critical security incident in terms of "immediate fear for the well-being [of various categories of persons]", the key work being 'immediate'. The Protocol assigns to the Security team the role of assessing the risk posed by individual security incidents and developing action plans to ensure an appropriate response. The Protocol also identifies an incident that can be "critical, but not urgent (or time critical)", when the management and acceptance of residual risk becomes the responsibility of the relevant senior executive officer via the reporting system.[22]

2.10 It is further noted that the Security team's processes in practice have evolved significantly from the procedure set out in the Protocol.

2.11 The conclusion is that the failure to distinguish between the responses required for different types of critical security incidents is a deficiency in the Department's security framework.

S 47E

[19] *Managing Critical Security Incident Protocol*, p. 2.
[20] It is noted that the PSPF (2018) does not refer specifically to clients who threaten self-harm. See PSPF, 15 Physical security for entity resources, p. 1.
[21] Interview, p. 2 and the Protocol, p. 5.
[22] *Managing Critical Security Incident Protocol*, p. 3.
[23] Interview, p. 15.

2.14 The Protocol was described to the Review as a 'live' document. Accordingly, it is reviewed as the need arises, not on a regular basis. At the present time, the Protocol is out of date, as was acknowledged to the review, from at least two perspectives. For example, in the light of changes in 2018 to the PSPF, the Protocol is being revised. It was also said to be "in the process of review because we've now introduced … the Triage [the Triage and Connect team] process into the [to the critical security incident response] system".[24]

2.15 The conclusion is that, if documented critical incident security procedure is to be reflected in practice, the *Managing Security Incident Protocol* (or its replacement) needs to be reviewed on a regular basis, at least annually.

Recommendation 1: That the *Managing Critical Incident Protocol* (or its replacement) be reviewed on a regular basis, at least annually.

How critical security incidents are handled

2.16 Critical security incidents are mostly identified by telephone, but can also be received in person, letter and by email. On the Department's intranet, there is an emergency tab which, when clicked on, brings up a security incident form which can be emailed to the Security team.

2.17 According to the critical security incident reference card, when a threat is imminent, the prescribed action for Department staff members is to call 000 and then report the incident to the Security team. In cases when the threat is not imminent, the prescribed action is to report the incident to the Security team.

2.18 The Protocol requires Department staff members to "immediately inform their manager about any activity or behaviour that could escalate to a critical security incident, report all security incidents to their manager and DVA Security using the security incident form or by telephone as soon as practically possible' and work with the Security team to manage incidents/critical incidents".[25]

2.19 When the Security team receives information about a critical security incident, it makes an initial assessment. As a result, it may implement "immediate controls that will either reduce the risk level [which] the threat provides or provide additional protection for DVA employees/members of the public".[26]

[24] Interview, p. 2.
[25] *Critical Security Incident Protocol*, p. 4.
[26] *Managing Critical Security Incidents*, p. 14. "Immediate controls can include: request for police or medical assistance; additional guarding for [an] individual tenancy; locking entrance doors; utilising 'move on' powers; staff evacuation; and meeting directives for high risk persons attending an office."

2.20 Subsequently, the Security team undertakes an investigation, followed by an assessment in accordance with Departmental risk assessment methodology, as identified in the Protocol, and the DVA Risk Management Framework. Ratings are assigned to 'likelihood and consequence' according to a risk assessment matrix (at Table A4 of the Protocol).[27] The assessment report outlines "what action has been taken, the current risk posed by the client" and contains recommendations. A residual risk level is also provided which "highlight[s] the Departmental assets that the risk effects – an individual, physical property, Departmental reputation or ICT security".[28] The Security team reports its assessment to directly affected staff and senior management.

2.21 In this context of responding to critical security incidents, the Security team regards its role as being the first point of call for risk management.[29]

Handling critical security incident responses involving a threat of client self-harm

2.22 In making an initial assessment when a client has threatened self-harm, the Security team contacts the staff member who submitted the incident report. The purpose of that contact was described to the review as follows.

> *[The] exact wording is critical for us to try and get … [a] picture of the state of … mind [of the client].*[30]
>
> *Why are they saying this? Is it claims related? Are they having issues with the Department? It's a … threefold thing. Looking first at what's the specific risk, is it imminent, is it serious, is something going to happen; secondly what was it – support for the veteran from a mental health perspective – so linking up with our [business] areas; and thirdly, from a claims perspective, looking at the business of the Department – what are we doing to assist?*[31]

2.23 In the first instance, the question which the Security team seeks to address is:

> *Are they in danger? What can [be done] to mitigate that risk?*[32]

[27] *Managing Critical Security Incident*, p. 14. See also Appendix A of this report.
[28] *Managing Critical Security Incident*, pp. 14-15.
[29] Interview, p. 4.
[30] Interview, p. 24.
[31] Interview, p. 4.
[32] Interview, p. 5.

2.24 The Security team can access its Security Incident Register (to check whether a client has come to notice before),[33] the client's medical history and records held on the Departmental Management Information System (DMIS), VIEW and the relevant business area(s) to ascertain progress of any current claim(s). The Security team can also contact the Triage and Connect team and Open Arms.[34]

2.25 The liaison between the Security team and the Triage and Connect team (and before that STAT[35]) has been developing for the past six to twelve months, a development which the Security team regards as very useful.[36] As stated to the review:

> *we can refer to them directly now and get a tangible benefit for the client, not just in reducing immediate risk, but also … in relation to their mental health with their claims. I think that's been … revolutionary, as opposed to just managing the risk...*[37]

2.26 When the Security team is unable to determine the level of risk, the review was informed that "at times…we get the business area to challenge the veteran…[S]taff members are encouraged to challenge them on their threats… And staff learn that through their ASIST training[38] and our support".[39] In this context, the Security team uses the term 'veiled threat'.[40]

2.27 It is noted that such an approach may not be consistent with best practice in relation to responding to client threat of self-harm. In addition, it could place inadequately trained staff members from the Department's business areas in an invidious situation.

2.28 If there is an immediate threat to the safety of a client, the Security team makes contact straight away with emergency services by calling 000 and requests a welfare check. The intention of such a request is for police or ambulance to attend. Occasionally, if the situation is already known, the Security team contacts police directly.[41]

2.29 The greater the risk of client self-harm, the sooner the Security team will contact emergency services.

---

[33] Interview, p. 9. For example, if the client were being case managed, the Security team could speak with someone who manages the client's case to obtain a picture of the background to the situation.
[34] Open Arms – Veterans and Families Counselling.
[35] Strategic Transformation Advisory Taskforce.
[36] Interview, p. 30.
[37] Interview, p. 24.
[38] ASIST is "a two-day interactive workshop in suicide first aid. Participants learn to recognise when someone may be at risk of suicide and respond in ways that help improve their immediate safety and link them to further help. ASIST aims to enhance participants' abilities to help a person at risk to avoid suicide". DVA Intranet. (It is noted that this site has not been updated since 2014.)
[39] Interview, p. 24
[40] Interview, p. 4.
[41] Interview, p. 23.

If it's determined that … there is a risk of self-harm, we'll go to emergency services first … then we gather up all the data and … pass it to the Triage and Connect team and [tell them] we've passed this to emergency services. Here's the background so you … can be doing what you need to do. We'll also give you an update once emergency services … calls us back.[42]

2.30 This approach places the Security team at the centre of the critical security incident response involving client threat of self-harm.

2.31 There were 475 critical security incidents recorded in the Security Incident Register during 2018. Of those incidents, 319 involved a reference to self-harm. Of those incidents, 62 involved support from emergency services. Of those instances of emergency services support, the Security team referred 38 incidents, with the remaining 12 incidents being referred by external parties.[43]

<u>Assessing and reporting critical security incidents</u>

2.32 As noted previously, the Security team assesses all critical security incidents and provides a report. The Protocol, which characterises this process as an investigation, states as follows:

At the conclusion of an investigation, the assessing officer should provide an assessment report to directly affected staff and senior management, outlining what action has been taken, the current risk posed by a client, as well as any recommendations for further action. A residual risk level should also be provided – this should be consistent with the Risk Assessment Matrix found at Table A4 [of the Protocol].[44]

2.33 It is noted that the risk assessment matrix, which the Security team uses to make its assessment, is seemingly oriented towards the risk of harm and damage to agency operations. However, it is also noted that the Protocol identifies a number of factors which the Security team must take into account and that "where a medical professional assesses a client as posing a particular threat to themselves, Security staff members must defer to expert opinion.[45] This statement provides the key to a revised approach.

[42] Interview, p. 5.
[43] Submission from the Security team.
[44] *Managing Critical Incident Protocol*, p. 14. The Risk Assessment Matrix is at Appendix A of this report.
[45] *Managing Critical Incident Protocol*, p. 13.

2.34 Although suited to incidents relating to damage, theft of property or compromise of official information, the review regards assessment reports based on the risk assessment matrix as being inappropriate or irrelevant to clients at risk of self-harm. Indeed, assessment reports which the Security team produce in relation to critical security incidents involving threats of client self-harm were described to the review as being 'roneoed'.[46]

2.35 It is not surprising that the review was told that the critical security incident assessment reports tended to be formulated from the point of view of the Department, not the client.

s 47F

2.36 A similar comment made to the review was that the Security team sometimes determined that the risk was low when the risk of harm to the individual might be quite high, suggesting again that the Security team assesses risk on the basis of risk to the organisation rather than the individual.[48]

2.37 The conclusion is that use of the risk assessment matrix is inappropriate in assessing and reporting critical security incidents involving client threat of self-harm.

<u>Does the Department have the correct setting for responding to critical security incidents involving client threat of self-harm?</u>

2.38 As noted previously, the critical security incident response reference card states that when faced with a threat of self-harm, and the caller states intent and advises the threat is imminent, the staff member in question is to call 000 and then report the incident to DVA Security.

2.39 The conclusion is that the critical security incident response reference card's guidance is dubious. All critical security incidents involving client threat of self-harm should be reported first to the Department's nominated point of contact. The decision about whether a critical security incident involving client threat of self-harm is imminent, and a call to 000 warranted, should not be left to individual staff members to decide.

2.40 **Recommendation 2: That Department staff members be required in the first instance to report all critical security incidents involving client threat of self-harm to the Department's nominated point of contact.**

[46] Interview, p. 3.
[47] Interview, p. 4.
[48] Interview, p. 2.

2.41 Concern was expressed to the review that a welfare check[49] may have an adverse impact on a client who has threatened self-harm. The review was told that, in managing risk effectively, having the police call on a client could exacerbate any anxiety that might be leading to high risk behaviour, rather than have a moderating effect.[50] Another comment was that the response to such a critical security incident requires consideration of who would provide the best support. For example, it may be a best friend or a general practitioner.[51]

2.42 It is noted however that, depending on the situation, a welfare check by police can be justified. For example, if it were assessed that a client who threatened self-harm had access to a firearm.

2.43 In effect, the Security team leaves it to 000 to decide, on the information which Security team provides, whether to send police, an ambulance or a Crisis Assessment and Treatment Team (CATT).[52] A comment made to the review was that, when a referral is made to emergency services under the current processes, responsibility for the incident is handed over. As a consequence, the Department's ability to manage the situation professionally is hampered and it is not clear who is managing the clinical risk.[53]

2.44 The review was told that, in the context of critical security incidents involving client threat of self-harm, the Department should enhance its relationship with State and Territory mental health services. The aim would be to develop partnerships, based on trust, so that when a Department clinician (including from Open Arms) made contact, the appropriate response could be obtained. Such partnerships could be based on a protocol and/or service level agreement so that a request for assistance would result in an agreed course of action for each client,[54] ensure the right level of care and enable the Department to manage the risk.[55]

2.45 The conclusion is that, consistent with the reorientation of the Department to achieve positive outcomes in its relationship with clients, new processes are needed to engage with those clients who threaten self-harm. The current approach of using the critical security incident response framework is no longer suited to meet this need.

[49] A welfare check may involve police calling on the client to check on the client's wellbeing.
[50] Interview, p. 5.
[51] Interview, p. 7.
[52] Interview, p. 14,
[53] Interview, p. 5.
[54] Note that the former Department of Immigration and Border Protection had MOUs with State and Territory Health Departments concerning payment for services to non-citizen asylum seekers.
[55] Interview, p. 16.

Recommendation 3: That the Department's current processes for engaging clients who threaten self-harm is no longer appropriate and that revised processes be developed based on a clinical framework and the involvement of clinicians.

Recommendation 4: That the Department develop partnerships with State and Territory mental health services as part of revised processes for engaging with clients who threaten self-harm.

Underlying issues: the Security team fills a vacuum

2.46 A comment made to the review was that the Security team's role in relation to critical security incidents involving client threat of self-harm results from a 'vacuum' caused by how the Department engages with its clients:

s 47F

2.48 That being said, the Security team was described to the review as being held in high-standing for the 'support' role its members play.[59]

2.49 As already noted, when a client indicates the possibility of self-harm, the incident is escalated to the Security team whose response is to handle it as a critical security incident in accordance with the *Managing Security Incident Protocol*.

2.50 The need for greater support for Department staff members is indicated because of "the changing nature of how we're going in terms of this additional engagement [with clients]".[60]

[56] Interview, p. 19.
[57] Interview, p. 12.
[58] Interview, pp. 12-13.
[59] Interview, p. 4.
[60] Interview, p. 6.

The Department is getting more and more complex matters come in. It's not that they never existed before, it's just that they were out there and the veterans didn't feel they had a voice, and the Secretary wants them to have a voice, and so how do we arm ourselves … with the right capability and capacity to be able to [give them support]. [W]e can get some really good resolutions, and I think we have.[61]

2.51 The Department's staff members need to have an increased level of positive engagement with clients. The requirement is for them to understand the principles of trauma-informed service delivery and ways of relating to people who are difficult, not because they're trying to be difficult, but because they may be unwell.[62] The requirement is also for staff training to include suicide awareness[63] and mental health awareness.

Recommendation 5. That Department review and revise its current suicide awareness and mental health awareness so that client-facing staff members are provided annually with face-to-face training.

2.52 The situation referred to above appears to reflect the historical lack of approach to the whole of person well-being, before the Transformation journey began.

[I]f you want to know something about a veteran, you have to consult a whole lot of different systems - maybe eight or nine have to be opened on double screens to be able to put a picture together of the things that are affecting an individual – that's really tough for staff to do. So this focus on trying to deliver better for veterans is quite difficult when you can't see what's going on. Different parts of the business would do their own thing, which would have an impact on the person, but weren't able to join themselves up to understand the overall impact on the individual.

And unwittingly … some difficult things would happen to people because of coinciding actions by different parts of the department, often unbeknownst… [T]here was a cultural issue with that, as well, and a fairly siloed and disparate style of operating…[64]

2.53 Another similar comment was made to the review, as follows.

…places like Child Support Agency or Centrelink … have a single client view system, so there's one system that has every single point of contact that the client has made with the department and, so, there'll be updates on there.[65]

---

[61] Interview, p. 6.
[62] Interview, p. 21.
[63] The Australian Defence Force provides instruction on this topic to its members as part of their mandatory annual awareness training. The suicide training (in face-to-face presentation format) could be adapted for use by the Department.
[64] Interview, p. 2.
[65] Interview, p. 29.

2.54 It is noted that the Department's Improving Processing Systems Program is addressing this key issue.

Demands on Security team members who handle critical security incidents

2.55 The Security team told the review that the handling of critical security incidents can place its members under significant pressure. As said to the review, some situations were described as being confronting. It was also said that:

> *[I]f something goes wrong, it could have quite severe ramifications.*[66]

s 47E t

s 47E . Support is also available from the Employee Assistance Programme.

2.57 The Security team told the review that, in relation to the critical security incidents it has managed, no client has committed suicide immediately following an incident that has been referred to it.[67]

Other processes used in the Department for responding to client threat of self-harm

2.58 Although the Protocol provides for client threat of self-harm to be referred to the Security team, other processes are also being used within the Department.

> *There's two different models at the moment, and that's a really important distinction to make … and then there's also a very different approach taken with the handling of the Secretary's caseload.*[68]

2.59 The review was informed that the Executive[69] has established the practice of working with the relevant business area which liaises with the Security team when necessary.[70] When there is a concern about the welfare of a client, liaison occurs with Open Arms, the Triage and Connect team and the Managed Access team.[71]

---

[66] Interview, p. 11.
[67] Interview, p. 24.
[68] Interview, p. 16.
[69] In this context, the Executive was then the Secretary, Commissioner, Deputy President and Chief Operating Officer.
[70] Interview, p. 11.
[71] Interview, p. 9.

2.60 There is another process which applies in the Department to incidents which would otherwise meet the definition of a critical security incident. This process has been adopted by Open Arms. Open Arms' approach to client threat of self-harm is that only senior clinicians contact and liaise with emergency services.[72] This approach is discussed in more detail at paragraphs 4.7-4.9 of this report.

Investigations

2.61 The Security and Investigations Section is responsible for investigations relating to fraud and information security. It also assists with investigations relating to public interest disclosure. See Chapter 5 for details relating to the Investigation team's resourcing, training, credentials and capability in relation to investigations.

[72] Interview, p. 4.

Chapter 2 – Consider the arrangements in place to ensure physical, personnel and information security (other than IT Security)

This chapter considers the arrangements in place relating to physical, personnel and information security (other than IT security) within the Department and the policies and documentation supporting these arrangements.

Security documentation

3.1 The Department has documents relating to its physical, personnel and information security arrangements. They are as follows:

- Protective Security Policy
- Agency Security Plan
- Risk Management Plan
- Bomb Threat Protocol & Checklist
- Information Security Protocol
- Managing Security Incident Protocol
- Physical Security Protocol
- Remote Duress Alarm Protocol

3.2 The Security team is responsible for these documents, which applied during the 2016-2018 period. The documents have been recently revised and redrafted for the purposes of the post 2018 period and the requirements of the revised PSPF, which the Department received in October 2018. The recent completion of this task is a significant achievement and the documents are currently awaiting endorsement.

3.3 To support the Secretary, the PSPF mandates the appointment of a Chief Security Officer (CSO) (at the senior executive service level) who is responsible for directing all aspects of security to protect the Department's people, information and assets. The CSO chairs and oversees a Security Governance Committee. The role of the Committee is to review security objectives, monitor performance and assess maturity compliance. It is the body through which the CSO manages those security responsibilities.[73] The establishment of the Security Governance Committee is pending.

[73] PSPF Changes Overview.

Information Security

Classified material

3.4 It was suggested to the review that a culture of complacency exists when the Department in relation to classified material. An example was cited of correspondence from the Prime Minister to the Minister for Veterans' Affairs being directed internally to the relevant business group, but not via the Secretary's office.[74]

3.5 In this context, it is noted that the Department has recently rolled out the DVA Protected Network – s 47E which provides for the secure digital transmission of sensitive documents.

> *The Commonwealth Protective Security Policy Framework (PSPF) states that the loss or compromise of **PROTECTED** information has the potential to cause damage to the national interest, organisations or individuals. To seek to protect the Department from the risk of this damage all electronic documents that contain **PROTECTED** information are to be handled within the DVA Protected Network - s 47E is administered for DVA by the s 47E]. It is a secure ICT environment with its own instances of desktop applications including Outlook, Microsoft Office products, PDMS and TRIM. s 47E is deliberately separate and isolated from the standard DVA (Unclassified) environment.*[75]

Safes

s 47E

[74] Interview, p. 5.
[75] https://intranet.dvastaff.dva.gov.au/supportingbusiness/minparl/Pages/Protected-Network-s 47E .aspx
[76] Interview, p. 2.

Clear desk policy

3.8 It is noted that the clear desk policy, required by the Department's Protective Security Policy, is adhered to in a haphazard way and is not enforced.

3.9 The conclusion is that such matters reflect adversely not only on the Department's security practices, but also indicate that its security culture may need to be reset. The Smith review of the Department of the Prime Minister and Cabinet's (PM&C) security procedures, practices and culture[77] is discussed later in this report. The need for a similar focus in the Department on security training and behaviours is pressing.

Recommendation 6: That the Department adopt the relevant recommendations of the Smith review in relation to security culture, training and behaviours, namely

- **the Secretary and Deputy Secretaries should lead in raising awareness and accountabilities for security**
- **All Canberra-based new starter staff members should be required to undertake face-to-face security training within the first week of commencing at DVA**
- **All regional new starter staff members should be required to complete mandatory online training within a week of commencement**
- **The effectiveness of the Department's security training [for current staff members] should be evaluated regularly**
- **Random internal security checks and periodic independent audits of staff security and the storage of classified information should be undertaken.**

<u>Chief Security Officer</u>

3.10 The requirement to consider the Department's security culture is a role for the positon of Chief Security Officer. At present, the Chief Security Officer is the FAS Legal, Assurance and Governance. This interim appointment reflects the functional responsibility for the Security, Governance and Quality Assurance Branch in which the Security team is located.

[77] March 2018.

3.11 As is clear from the Smith review, the required emphasis in relation to security is on culture. It is noted that PM&C's transformation agenda is to embrace innovation and build a technologically aware, digitally enabled and data-driven workforce. This emphasis on digitisation and security culture leads to the need to consider the First Assistant Secretary (FAS) Business Support Services position as being the most suited to perform the role of Chief Security Officer. As the Chair of the People and Culture Committee, and head of the Division in which the Business Integration and Analysis Branch (IB & AB) is situated, the FAS Business Support Services position brings together the necessary elements to develop the Department's security culture, namely people, digitisation and training.

3.12 The conclusion is that the FAS Business Support Services should be appointed as the Department's Chief Security Officer.

Recommendation 7: That the FAS Business Support Services be appointed as the Department's Chief Security Officer.

<u>Cabinet documents</u>

3.13 The review was told that a lack of discipline is evident concerning the distribution of Cabinet documents. Proper practices in relation to such material are an important sub-set of information security. Although digitisation is underway, the Department has a significant way to go. As that process continues, the digitisation of every task cannot be expected and some paper documentation will persist. Hence, the requirement will remain for classified information to be created, printed, and stored in traditional ways.[78]

3.14 The review was told that the Parliamentary and Executive Support Branch and the Security team have not always been aligned in relation to the handling of Cabinet documents. However, the current close working relationship is noted.

> *We're responsible for Cabinet documents … but they [the Security team] provide the security advice on the handling of any classified … information. And so, there's that crossover. … Because they're ultimately providing advice in relation to what's changed with the Protective Security Framework, we have to comply with that as well as the guidelines set out in the Cabinet handbook…It creates a complexity…where it was our view and interpretation of the Cabinet handbook … that something's classified ... Security would give … different advice. But we've resolved that and it hasn't come up in recent months.*[79]

[78] Smith review, p. 16.
[79] Interview, pp. 21-23.

3.15 The conclusion is that there must be explicit understanding between the Parliamentary and Executive Support Branch and the Security team in relation to the handling of Cabinet documents. It needs to be clear who is responsible for the policy relating to the security of Cabinet documents.

Recommendation 8: That the Secretary issue a delegation or direction to the Assistant Secretary Parliamentary and Executive Support to be responsible for all aspects relating to the handling of Cabinet documents, including security policy.

Recommendation 9. That, noting the recommendations of the Smith review (of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture), the Department develop a training and information package to increase awareness and understanding among its staff members about Cabinet document handling and storage.

Security of clinical records

3.16 It is noted that Open Arms' clinical records are kept independently from the Department. They are on a separate server in a different cloud. Open Arms also has clinical records in hard copy form. The Security team provides advice to Open Arms on how those records should be stored, although Open Arms has the responsibility for them.[80]

IT Security

3.17 The review's terms of reference state that "[t]he review will consider arrangements in place to ensure physical, personnel and information security (other than IT Security)." The Business Integration & Analysis Branch (BI & AB) told the review that it regards information security as being fundamentally connected with IT Security.

3.18 BI & AB's view is that it would be challenging to understand how information is protected without considering the technical controls relating to that protection. Other aspects of IT security and technical implementation are also relevant, for example the governance, policies and procedures can affect the effectiveness of Information Security.

3.19 BI & AB is aware of the size and complexity of IT Security as a topic and suggests that it be reviewed subsequently.

3.20 It is noted that the Security team and BI & AB are currently drafting a document to meet the requirements of the revised PSPF and the Information Security Manual.

[80] Interview, pp. 14-15.

3.21 BI & AB told the review that it is not aware of any team in the Department that could conduct investigations across the range of potential event scenarios. While an internal audit area would have similar engagement methodologies, placement of the capability in the 'Internal Audit Subsection' may not be reasonable if the subsection does not have the skillset. According to BI & AB, the Department will need to build the capability and either hire resources with the required skillsets, or assist existing resources in upskilling in appropriate investigation and coordination skills. [81]

Security in the context of outsourced service delivery functions

3.22 Reference was made earlier in this report to the Department's future operating environment. (See paragraph 1.8.) In that context, possible extension of arrangements with organisations like the Department of Human Services would involve physical and information access. Such access raises issues about how the Department would manage and assure itself about any associated security risk. For example, this situation would require input from the Security team about such aspects as security clearance levels.[82]

3.23 Integration in the context of outsourced service delivery functions raises other issues when there may be different standards between the integrated entities. For example, in the case of shared premises, the Department may show more tolerance in relation to behaviour when seeking to engage with clients than DHS where there may be a lower tolerance.[83]

3.24 The Department's response to the revised PSPF will need to take into account the security risks associated with outsourced and integrated service delivery functions.

[81] Submission made to the review by the Business Integration and Analysis Branch, emails dated 15 & 16 January 2019.
[82] Interview, pp. 16-17.
[83] Interview, pp. 18 & 20.

s 47E

s 47E

s 37

s 47E

s 47E

s 47E

s 33, s 47E

[107] Department of Veterans' Affairs, *Annual Report 2017-18*, p. 75.

s 33, s 47E

[108] Interview, p. 5.

s 33, s 47E

Chapter 5 – Consider the appropriateness of the Security and Investigations Section's resourcing, training, credentials and capability compared to Australian Public Service (APS) agencies with a similar function

This chapter considers matters relating to the operation of the Security and Investigations Section, including resourcing, training, credentials and capability, and compared these matters to APS agencies with a similar function.

6.1 In addressing this criterion, the review consulted with representatives of the Australian Taxation Office and the Department of Human Services (DHS). It is noted that DHS has three programs: Centrelink; Medicare; and Child Support.

S 47E

Security team functions

6.4 The Security team performs a number of functions: protective security; personnel security; and critical security incident management. It is on call 24 hours, 7 days a week to respond to critical security/physical security incidents.

Protective security

6.5 The Security team, which is based in Canberra, is responsible for the Department's physical security, which includes such measures as access cards, mobile and fixed duress alarms, alarm monitoring, safes/security containers and access controls.

6.6 Site reviews and annual risk assessments are conducted of all Departmental tenancies (domestic and international). Physical inspections take place bi-annually to ensure that appropriate security measures are in place.

6.7 The Security team provides security advice and support in relation to commemorative and other events held internationally and in Australia. For that purpose, the Security team liaises with law enforcement, intelligence and security agencies and other relevant government bodies.

6.8 Face-to-face security awareness training for the Department's client-facing staff members is provided by the Security team, which is also responsible for mandatory on-line security training.

Personnel security

6.9 The Security team manages security clearances within the Department and liaises with the Australian Government Security Vetting Agency (AGSVA). The Department's staff members with access to sensitive information or systems are required to hold a security clearance as outlined in the Protective Security Policy.

Critical security incident management

6.10 The processes for responding to critical security incidents are described at paragraphs 2.16-2.21 of this report.

Information security

6.11 The Security team distinguishes between a critical security incident and a serious security incident. A serious security incident refers to the situation when a leak of classified document or a breach of an IT system occurs, as defined by the PSPF. The review was informed that the Security team has not investigated a serious security incident for two or more years.

Security team workload

6.12 The number of critical security incidents handled by the Security team is provided below at Table 3.

Year	Critical security incidents	Referrals to emergency services
2018	475	62
2017	334	65
2016	283	60
2015	344	70

Table 3 – Number of critical security incidents

s 47E

Unreasonable Client Conduct

6.14 The Security team provides advice about unreasonable client conduct and for that purpose liaises with Managed Access, Coordinated Client Services and Open Arms.

Investigations team

s 47E

6.16 Investigations are conducted in accordance with the Australian Government Investigation Standards (AGIS) and the Commonwealth Fraud Control Framework. There is an Investigation Manual which outlines the procedures to be followed.

6.17 All allegations relating to fraud are recorded in a centralised Fraud Case Management Information System (FCMIS) and assessed against a case prioritisation model to determine if criminal investigation is warranted.

6.18 The Investigations team serves as the point of contact for business areas and the public relating to allegations of fraud against the Department. Such allegations relate predominantly to veterans' benefits and health provider claims.

6.19 The review was informed that most allegations which the Investigations team receives relate to client fraud, whereas most investigative effort relates to provider fraud.[114]

Investigations team workload

6.20 The investigation team estimates that it devotes 95% of its time and effort to conducting fraud investigations. The remaining time is spent with investigations under the *Public Interest Disclosure Act 2013* (the PID Act) and Australian Public Service Code of Conduct under the *Public Service Act 1999*.

6.21 Information about the Investigations team's fraud work is provided in the following table.

	FY 2017-18	FY 2018-19 (to date - 4 Feb 2019)
Cases on hand at beginning of FY	135	107
Cases received in FY	337	208
Matters before the Courts	1	1
Matters referred to Commonwealth Director of Public Prosecutions or law enforcement agencies	0	1 (pending)
Convictions	0	0
Finalised Cases	365	208
Cases on hand at end of period	107	107

Table 4 – Statistics relating to fraud investigations

Resources

Security team

s 47E

[114] Interview, p. 18.
[115] Interview, pp. 13-14.

s 47E

s 47E

s 47E

s 47E

s 47E

s 47E

APS Agencies with a similar Security and Investigations function

Australian Taxation Office

6.52 The ATO has established a Security Intelligence Unit (SIU), which commenced in February 2019. The SIU is headed by a Security Intelligence manager at the EL 1 level, who will report to the ATO Agency Security Adviser (ASA), which is an EL 2 position.

6.53 The ATO addresses the issue of security by identifying several categories which are: physical security (under ATO Property); personnel security (under Human Resources); and information and cyber (under Enterprise Security Technology).

6.54 These various focuses on security are coordinated by the Security and Business Continuity Management Committee, which comprises Band 2 level officers, and a Security Sub-committee, which comprises Band 1 officers chaired by a Band 2.

6.55 The ASA is concerned with physical security. There is also a Chief Security Officer (at the Band 2 level). The ATO has a dedicated PSPF compliance unit.

[133] See P. Moss, *Statutory Review of the Public Interest Disclosure Act 2013*, July 2016, p. 7. "Recommendation: To strengthen the PID Act's focus on significant wrong doing like fraud, serious misconduct, and corrupt conduct in order to achieve the integrity and accountability aims. To this purpose, personal employment-related grievances would be excluded from the PID Act, unless they relate to systemic issues or reprisals, and 'disciplinary conduct' would be defined as termination or dismissal. Such issues are better dealt with or resolved through other existing dispute resolution processes."

6.56 The work performed by the ATO is changing, for example more of its staff members work remotely. There is also increasing focus on compliance and terrorism financing. The Black Economy Taskforce works in the community by making visits to businesses. In this context, the major security challenge for the ATO is the protection of its staff members.

6.57 The digital environment is also having a significant impact on ATO staff members. Sometimes incidents occur of on-line aggression, harassment and targeting that can cross over into private life. From time to time, ATO clients attempt to contact ATO staff members through personal channels.

6.58 Unlike DVA, the ATO is not in a care role for its clients. When an ATO client makes a threat of self-harm, the ATO response is to report the matter to the police. No other action is considered necessary. However, this approach is changing.

6.59 The ATO maintains an interest in threats of harm against others. In the past, the ATO engaged a private firm, Code Black, which is a threat management consultancy based on forensic and psychological diagnosis. The ATO is currently developing its own threat management capability through the SIU, which is being advised by another private firm, New Intelligence.

6.60 The SIU will meet the need in the ATO to have a centralised function for security and intelligence. At present, there is no centralised knowledge of risk, or point of contact for business areas, when dealing with complex clients. Business areas themselves do not have the necessary capability.

6.61 The ATO is exposed to risk. It has accepted that comprehensive understanding of the risk spectrum and threat needs to be developed, a need which can be hampered by such factors as 'patch protection' or its siloed organisational structure, and a failure to routinely record incidents across the agency as normal business practice.

6.62 Fixated Threat Assessment Centres (FTAC) have been established by State and Territory law enforcement agencies. These centres are based on joint policing and mental health strategies. SIU is in the process of setting up pathways with FTACs, recognising that a punitive response is not always appropriate.[134]

6.63 The conclusion is that the ATO is developing its threat management capability and enhancing the security measures for its staff members by centralising its knowledge relating to risk. The Department and the ATO could learn from each other's experience.

[134] Meeting with ATO Security Intelligence Unit Manager designate, 11/2018.

s 47E

[135] DHS, p. 2.
[136] DHS, pp. 2-4.
[137] DHS, p. 16.

6.70 The conclusion is that the Department and DHS are engaging similar issues in relation to client threat of self-harm and could learn from each other's experience.

[138] DHS, p. 9.
[139] DHS, p. 11.

Chapter 6 – Consider the implementation of the recommendations from the Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture

This chapter considers what actions DVA has undertaken following the review of the Prime Minister and Cabinet Department's Security Procedures, Practices and Culture. In particular, the focus is on DVA 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.

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

7.1 On 31 January 2018, 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, reported following the purchase of locked filing cabinets at a second hand furniture shop in Canberra. It was confirmed that the documents came from within the Department of the Prime Minister and Cabinet (PM&C).[140]

7.2 An independent review of PM&C's security procedures, practices and culture was conducted by Mr Ric Smith. The review, which reported in March 2018, made a number of recommendations that were relevant to both PM&C and the wider APS.

7.3 The Smith report recommendations relating to PM&C are listed under the following headings: operating environment; protective security governance arrangements; documented practices, systems and procedures; and culture, training and behaviours.[141]

7.4 The Smith report noted that failings of a similar nature have occurred in other departments and agencies and are probably systemic in the APS. The recommendations relating to the APS are as follows.

- **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.**

[140] Smith Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture, March 2018, p. 5.

[141] Smith Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture, pp. 8-9.

- **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.**
- **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.**
- **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.**
- **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.**
- **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.** [142]

7.5 In response to the Smith report, the DVA Security team conducted a review of the Department's safe disposal processes. This work included a stocktake of all safes and lockable cabinets. The outcome, as reported by the Security team, was that the Department's safe disposal processes are robust, that classified material is handled safely and that all safes are recorded in a central register with the Security team and that an audit of all safes is undertaken upon relocation.[143]

7.6 Subsequently, doubt has arisen recently about the effectiveness of current procedures by the revelation reported to the review that the annual checks concerning the location of safes have not been undertaken for some time. (See paragraphs 3.6-3.7 of this report.) A comprehensive survey of safes is currently underway to remedy the situation.

[142] Review of the Department of the Prime Minister and Cabinet's Security Procedures, Practices and Culture, pp. 10-11.

[143] Interview, p. 30 and DVA Back Pocket Brief dated October 2018, Safe and Secure Disposal Arrangements for Safes and Secure Cabinets.

7.7 As reported to the review, the Security team has focused on security culture in line with the Smith review recommendations through drafting the response to the PSPF and providing training. In that context, the Security team is creating strategic and operational work plans to implement the PSPF changes, updating its policies and protocols to align with the PSPF and creating educational material to communicate the key components of the PSPF to staff members.[144]

7.8 The conclusion is the Department's response to the Smith review recommendations has been minimal. Instead, the Security team's focus has been on responding to the need to develop the Department's response to the revise the PSPF. As noted, this task is significant and has absorbed the Security team's focus and resources.

7.9 The conclusion is also that the Department needs to focus on the Smith review recommendations in a comprehensive and systemic way. This focus should come from the Security Governance Committee, when established, and the Security team. The claim that "we [have] done everything that was required of us, as an agency, as a result of the recommendations of the Smith review" is unwarranted.[145]

7.10 The conclusion is further that the focus should not only be to implement the Smith review recommendations for the APS, but also, with the necessary changes being made, recommendations relating to PM&C. (See paragraph 3.9 of this report.)

Recommendation 19: That the Department give priority to implementing the recommendations of the Smith review (into the Department of the Prime Minister and Cabinet's security procedures, practices and culture) and engage in a systematic and comprehensive response to it with a view to integrating those recommendations into its own security procedures, practices and culture.

[144] PSPF Changes Overview brief.
[145] Interview, p. 11.

Chapter 7 – Consider the appropriateness and effectiveness of the Department's Unreasonable Complainant Conduct (UCC) Framework and the role of the Client Liaison Unit

This chapter discusses the origin and the appropriateness of the UCC Framework and the development and approach of the current Managed Access Client Coordination Program.

Documentation relating to the Unreasonable Complainant Conduct Framework

8.1 The Department's website describes the Unreasonable Complainant Conduct Framework (the UCC framework) as multi-faceted, consisting of policy and guidance materials, procedures and tools for staff that have been largely adapted from materials developed by the Commonwealth Ombudsman and NSW Ombudsman offices. The website also states that "the UCC policy has been developed to assist all DVA staff members to better manage unreasonable complainant conduct".[146]

8.2 According to the Department's website, a very small number of clients require intensive management due to their unreasonable conduct when dealing with the Department. Such conduct includes threats to staff, abusive and offensive communications and unreasonable persistence and demands.

8.3 Also, according to the Department's website, when the UCC Framework was endorsed in October 2015, it was recognised that "persistent and unreasonable complainant behaviour is an issue that affects government agencies and personnel within them. Due to its dealings with individuals' personal affairs and high levels of direct client contact DVA is susceptible to UCC".[147]

8.4 The application of the UCC Framework is guided by a policy statement, which dates back to September 2015.[148] The UCC policy was issued by the then Secretary, yet the review could not obtain a signed copy.

8.5 The UCC policy sets out the objectives, defines unreasonable complainant conduct, roles and responsibilities, and alternative dispute resolution procedure to be followed "when changing or restricting a complainant's [client's] access to our services". The introduction refers to the Department being shaped by its strategic themes of being client-focussed, responsive and connected.

[146] DVA website: https://intranet.dvastaff.dva.gov.au/supportingclients/clientrelationshipmanagement/Pages/UnreasonableComplainantConduct.aspx
[147] Ibid, DVA website.
[148] DVA Unreasonable Complainant Conduct Policy – September 2015.

8.6 The UCC policy also refers to strategies that make it easier for clients to work with the Department, "by ensuring that we are responsive to all groups of clients, across all areas of our business and ensure a coordinated and consistent approach to delivering services into the future".[149] It is noted that while these opening words reflect the aims of the Transformation journey, the UCC policy which follows them does not.

8.7 The UCC policy is based on the Ombudsman *Managing Unreasonable Complainant Conduct - Practice Manual*.[150] It is noted that the use of language in the UCC policy changes after the first few paragraphs from 'client' to 'complainant'. It was explained to the review that this approach is justified because the policy is a direct copy from the Ombudsman practice manual.[151]

8.8 The use of terminology is important. To refer to particular clients as complainants indicates a kind of metamorphosis to a different status. It certainly suggests a warning or alert attaching to a given client. Accordingly, it is an unfortunate label which has been applied to certain clients by adopting the Ombudsman practice manual without appropriate adaptation and modification.

8.9 Everyone who seeks assistance from an Ombudsman is a complainant. That is universal Ombudsman terminology and is reflected in the Ombudsman practice manual. As to the Department, the relevant term for a veteran who seeks a benefit and assistance is 'client'. Accordingly, a better approach would be to use a description which encapsulates the notion of "a client who has been identified as raising concerning issues and who needs additional support"[152], for example a 'supported client'.

8.10 It is available to any client to make a complaint about 'a matter of administration',[153] both to the Department (about the Department) and to the Commonwealth Ombudsman (about the Department). For the UCC policy to use phraseology which connotes a different status for a veteran, other than as a client, and to link the making of a complaint with unreasonable conduct, is inappropriate. It diminishes the policy's effectiveness, causes confusion and is contrary to the aims of the Transformation journey.

---

[149] DVA: Unreasonable Complainant Conduct Policy, p. 1.

[150] *Managing Unreasonable Complainant Conduct - Practice Manual*, 2nd edition, May 2012. (The New South Wales Ombudsman, supported by all other Australasian Parliamentary Ombudsman, commenced a joint project to address the problem of chronic or overly persistent complainants and the disruptive effects of their conduct on public resources. The project sought to minimise the often disproportionate and unreasonable impacts of UCC on public sector organisations, their staffs, services, time and resources by proposing a framework of strategies for managing such conduct.)

[151] Interview, p. 23.

[152] See the Triage Referral Indicators, p. 1.

[153] *Ombudsman Act 1976*, section 5(1).

8.11 It is concluded that the UCC Framework policy needs to be revised to remove any possible misunderstanding or doubt about the Department's commitment to assist all veterans (as clients) and their families.

Recommendation 20: That the Unreasonable Complainant Conduct Framework policy be revised to remove any possible misunderstanding or doubt about the Department's commitment to assist all its clients and their families.

Background to the former Client Liaison Unit

8.12 The UCC Framework is administered by the Managed Access team, which is part of the Client Coordination and Support Branch. Previously called the Client Liaison Unit (CLU), Managed Access commenced in September 2018. The name change to Managed Access occurred in association with a Departmental restructure in July of that year.[154]

8.13 The CLU was established in 2007 for clients whose cases were complex, whose relationship with the Department had become untenable or significant behavioural issues were evident.[155] In 2016, the Coordinated Client Support Program (CCS) was established and located with the CLU. Recently, the CCS and Managed Access have been re-arranged, each with its own Director.

8.14 Now part of the Client Support Framework, the CCS provides clients with three levels of support, according to their needs. It is noted that Triage and Connect, which is also part of the Client Support Framework is the entry point for referral to CCS.[156]

The UCC Framework

8.15 The UCC Framework works with clients who may have the same risks and vulnerabilities as those referred to CCS. Those risks and vulnerabilities may include transition, relationship breakdown, substance abuse and/or homelessness. In some cases, protective factors such as medical, family or social support are limited or non-existent.[157]

8.16 Clients referred to Managed Access have demonstrated unacceptable behaviour in their dealings with the Department. Accordingly, UCC Framework clients' access to the Department is restricted to Managed Access. The UCC Framework is involuntary.[158]

[154] Interview, p. 1.
[155] Interview, p. 7.
[156] DVA website.
[157] Interview, p. 10.
[158] Interview, pp. 10-11.

8.17 The process for a client to be placed under the UCC Framework was described to the review as a graduated process. When unreasonable behaviour occurs, as defined in the UCC policy,[159] a written warning can be issued to the client. If the unreasonable behaviour continues, a notification letter can be issued. Continuation of the unreasonable behaviour can lead to referral to Managed Access. In some cases, the Security team recommends that a client be referred to Managed Access.[160] The UCC policy sets out in detail the restrictions that can be applied to clients.

8.18 The conclusion is that the UCC policy reflects a previous era of the Department's understanding of and approach to client relations. It is noted that, during 2017-18, Internal Audit Services conducted an audit of the UCC Framework. The outcome was that certain actions were suggested, including revision of the policy statement to reflect the operation of the UCC Framework in practice.[161]

8.19 From the Department's perspective, the issue has been seen as a workplace health and safety risk to staff members. It is an acknowledgement of the need to protect staff members. However, a comment made to the review was that the emphasis was more on the need to protect staff members than recognising a "damaged [client] who needs help".[162]

8.20 A view expressed to the review is that the UCC Framework is a very good mechanism, provided it is used sparingly.

s 47F

8.21 This view is expressed on the basis that Department staff members/delegates need to have conversations with clients to resolve issues at the lowest possible level and escalating to the next level only when there is a breakdown of communication or an inability to undertake what the client wants. Such an approach requires high value relationships with the client, even in trying circumstances.[164] It also requires Department staff members with the right training and culture.

---

[159] See Department of Veterans' Affairs: Unreasonable Complainant Conduct Policy, Unreasonable Behaviour, p. 5.
[160] Interview, p. 15.
[161] Internal Audit Services (KPMG) 2017-18, Review of Unreasonable Complainant Conduct Framework, 31 October 2018, p. 11.
[162] Interview, pp. 11 & 13.
[163] Interview, p. 22.
[164] Interview, p. 22.

8.22 From the client perspective, the comment made to the review was that referral to the CLU was regarded as 'DVA's naughty corner'.[165] [166]

s 47F

8.23 An example of the client frustration was provided in July 2018, when the Commonwealth Ombudsman[168] reported on the actions and decisions of the Department of Veterans' Affairs in relation to Mr A. The Ombudsman commented that "the sustained and continuing errors and resulting actions had a profound impact on Mr A's financial, physical, psychological and emotional state".[169]

8.24 A view expressed to the review is that the existence of the UCC Framework reinforces the perception that the Department is difficult to deal with. It is said to reflect the attitude of some staff members that there are advocates and clients who are just 'trying it on' in an attempt to gain unwarranted outcomes. In this context, Department staff members were described in some cases as being 'driven into a bunker'.[170]

8.25 Another view expressed to the review was that:

s 47F

8.26 Some clients may feel that their contact with the Department is segmented as their case file is passed progressively from one business area to another. It is a situation which is likely to add to any pre-existing sense of frustration.

[165] Interview, p. 19.
[166] The review was told that this term is used by the veteran community, Interview, p. 19.
[167] Interview, p. 19.
[168] In the role of Defence Force Ombudsman.
[169] Commonwealth Ombudsman, Investigation of the actions and decisions of the Department of Veterans' Affairs in relation to Mr A., July 2018, p. 15.
[170] An in-confidence submission to the review.
[171] Interview, p. 11.

Managed Access' Resources and Approach

s 47E

8.28 The approach which Managed Access adopts is to engage and build rapport with its clients. The intention is to try and resolve the matter relating to the cause of the referral under the UCC Framework. Accordingly, Managed Access staff members conduct most of their work by telephone because experience has shown that the use of email is not conducive to good communication with clients.[172]

8.29 There are currently about 66 clients who are subject to the UCC Framework. The review was told that there were 91 clients in 2017. That number has been reduced by systematic review of those clients' cases. Clients have been transitioned out of Managed Access when their behaviour in question has been resolved.

8.30 Although it is not the Department's stated policy, it is a priority for Managed Access to ensure that the UCC Framework is applied properly and carefully to clients. The result has been a reduction in the number of clients.

8.31 The UCC Framework requires clients to be reviewed every three, six or twelve months, depending on the nature of the unreasonable conduct and the service provided.[173] Following a Commonwealth Ombudsman recommendation, Managed Access has adopted the practice of reviewing each client at a minimum of every three months.

8.32 The process involves systematic review of the engagement within the preceding three-month period. Clients are advised by telephone and invited to make a submission. The result can theoretically include increased restriction, no change, transfer to business as usual or transition to CCS for which there is a streamlined arrangement to allocate a coordinator in a Managed Access location.[174]

8.33 Managed Access has developed its Guiding Values to reflect the coordination and support offered to clients despite the application of a managed point of contact. When coupled with updated job descriptions and recent staff recruitment, these guiding values have set new benchmarks and expectations in relation to how Managed Access works with unreasonable client behaviours.[175]

---

[172] Interview, p. 4.
[173] Department of Veterans' Affairs: Unreasonable Complainant Conduct Policy, Unreasonable Behaviour, p. 15.
[174] Interview, p. 18.
[175] Managed Access submission to the review (7 February 2019).

8.34 Since October 2018, following a recommendation of an Internal Audit review report,[176] Managed Access has been developing an advisory role. The aim is to provide support to business areas interacting with clients who may be displaying unreasonable conduct. This initiative was established in response to an increasing number of referrals being received by Managed Access. These referrals were being declined due to an absence of warning or attempts to address the client issue within and by business areas.

8.35 The requirement to warn and request modification following unreasonable behaviour is UCC policy. Only after the necessary steps have been taken can Managed Access consider accepting a referral.[177] Hence, proper management of unreasonable client conduct in the first instance can avoid the need subsequently to impose access restriction on clients.[178]

8.36 Since the implementation of the advice line program, Managed Access has been consulted on 10 cases, none of which has progressed to a referral to, or acceptance of, a client under the UCC Framework. This data - while reflecting an early stage – indicates a significant improvement compared with previous CLU statistics.[179]

8.37 Managed Access staff members told the review of their observation when delivering training that there is a skill gap in client-facing staff members in business areas about how to converse with clients. They noted "a nervousness and a lack of confidence [in relation to] those particular communications... [T]he tolerance for unreasonable client conduct is quite low ... [as is] engaging with clients who might have mental health conditions".[180]

8.38 Since Managed Access has published its advice line, it has seen an increase in requests for advice and a reduction in referrals. This result is attributed to staff members contacting Managed Access earlier and managing behaviour within their business areas more than previously.[181]

8.39 In this context, Managed Access maintains regular contact with the Commonwealth Ombudsman's office, which also provides training to Department staff members. Such training needs to introduce a feedback loop to the UCC Framework to assist the Department to understand why clients' conduct becomes 'unreasonable' and to help in the development of prevention strategies.

[176] The Internal Audit Report suggested that Managed Access undertake training and other communications activities to raise awareness of the UCC Framework as a tool for business areas, p. 11.
[177] Managed Access, submission to the review.
[178] Interview, pp. 5-6.
[179] Managed Access submission to the review.
[180] Interview, p. 9.
[181] Interview, p. 10.

8.40 The conclusion is that Managed Access is achieving best practice. It is arriving at this outcome by restoring the relationship with a number of UCC Framework clients, through systemically reviewing the need for clients to enter, and remain under, the UCC Framework and by supporting and advising Department client-facing staff members about dealing with unreasonable client conduct in order to reduce the need for and incidence of referral under the UCC Framework.

Recommendation 21: That the Department continue to reduce the number of clients under the Unreasonable Client Conduct Framework.

Recommendation 22: That the Managed Access advisory service be developed further as a resource to assist and support the Department's client-facing staff members.

Recommendation 23: That the UCC Framework be comprehensively revised, including its nomenclature, to reflect current Managed Access practice.

8.41 The conclusion is also that Managed Access approach could be expanded and applied more broadly. In order to restore the relationship with clients under the UCC Framework, and other clients who are disaffected, an approach needs to be developed which would be proactive and draw the line on past negative experience, some of which may have its origin prior to contact with DVA. Such an approach would involve a framework in which there is a commitment to understand the client experience and to respond in a meaningful way so as to bring closure for the client. The idea has been described to the review as a restorative justice approach,[182] but it could also involve the use of conciliation.

Recommendation 24: That the Department aim to restore the relationship with disaffected clients, both under the UCC Framework and beyond, by establishing a program which is committed to developing understanding of the client's past negative experience, developing trust and providing such a response as to bring closure for the client.

8.42 A comment made to the review about the challenges inherent in the work which Managed Access staff members undertake, was as follows:

It's a tough job and the individuals there take a fair amount of abuse…to get to a point where they can have a relationship with that client and progress whatever the issue is for the person. Until we get that relationship happening the issues do not … progress.[183]

8.43 The conclusion is that Managed Access staff members need to be provided with the support they require.

[182] Interview, 27/2/2019.
[183] Interview, p. 23.

8.44 A comment made to the review was that some client-facing Branches have the potential for greater incidence of unreasonable client conduct.[184] For example, interaction with the Client Benefits Division may cause distress or disquiet to clients. These Branches are the Primary Claims Branch and the Incapacity and Permanent Impairment Payments Branch. The business areas in these Branches have functions relating to initial liability, permanent impairment and incapacity. Once initial liability is accepted, a claim can be made to incapacity payments and/or permanent impairments. These business areas are the gateway to other services. The review was told that most other business areas are operational and may cause less contention.[185]

8.45 The review sought detailed information on the above topic, but it did not become available. The question posed was of the clients currently under the UCC Framework, how many were referred from each of the relevant business areas. Such information would be useful in the determining the need for client-facing staff training.

8.46 A comment made to the review was that:

> *All officers likely to be interacting with clients should have … training before they're allowed to directly interact with clients, and the Department should work with experts in the mental health issue[s] to develop a set of simple indicators such as frequent calling, non-responsiveness to help them [to] identify the behaviour that we're concerned about.*[186]

8.47 The conclusion is that the Department needs to develop a concentrated focus on providing its client-facing staff members with the skills and training needed to achieve optimal outcomes.

Recommendation 25: That the Department develop a concentrated focus on providing its client-facing staff members with the skills and training needed to achieve optimal outcomes for clients.

8.48 The Productivity Commission Draft Report notes that the need for policy which anticipates crises before they occur and making changes in the long term interest of veterans instead of policy change that is reactive.[187]

[184] Interview, p. 22.
[185] Interview, p. 8.
[186] Interview, p. 12.
[187] Productivity Commission, Draft Report, *A Better Way to Support Veterans*, December 2018, p. 445.

8.49 In this context, progress is being made. For example, the Legal, Assurance and Governance Division has listed clients who are engaged, or about to engage, in CDDA and AAT cases. It is noted that proposed legal action is one indicator of escalation. Another indicator may be the length of time it takes the Department to make a decision or when a client is denied a benefit. Such indicators are likely to exist across the Department's business areas. The need is for the Department to deal proactively with the possibility of escalation once such indicators are comprehensively and systematically mapped.[188]

8.50 The conclusion is that the Department needs become more predictive by developing the capacity to identify in a comprehensive and systematic manner the indicators which result in client escalation.

Recommendation 26: That the Department develop the capacity to identify in a comprehensive and systematic manner the indicators which result in client escalation.

8.51 This situation brings into the focus the issue of risk and how it is assessed. A comment made to the review was that in the Department the use of language around risk is imprecise. What is needed is a consistent approach to how risk is defined. There is also a need for improved risk identification and clear handover of risk management. Managing risk has to understood and become part of everyday business.[189]

s 47F

8.52 The review is aware that there is interest and intention among some senior executive leaders to develop a consistent approach in relation to how risk is defined in the Department. It is an initiative which is both worthwhile and necessary.

[188] Interview, p. 21.
[189] Interview, p. 2.
[190] Interview, pp.2-3.

Chapter 8 - Other matters relating to the Department's security and investigations functions

This chapter raises no additional matters.

Conclusion

9.1 A number of conclusions are made throughout this report. However, here is a summary of the key conclusion.

9.2 The Security and Investigations Section has core functions relating on the one hand to physical, personnel and information security and on the other hand to fraud investigations. They are undertaken in a similar way to any other Commonwealth department and agency. In DVA, these functions are augmented by the responsibility for critical security incidents involving client threat of self-harm and for the security arrangements relating to annual commemorative events held overseas.

9.3 These additional functions are a significant responsibility which the Security and Investigations Section performs well. Nevertheless, they are a seeming distraction. The recommendation is that these functions should be transferred elsewhere. This step would enable the Security and Investigations Section to concentrate on its core functions and free up the resourcing it needs to undertake them.

s 47E

Table 5– Risk assessment matrix.

2.63 The actions that the security team undertake between receiving the notification of the *critical incident* and finalising the report into the incident are outlined in the 'Managing Critical Security Incident Protocol'.

2.64 This assessment leads to a report into the incident. It provides a summary of the circumstances of the incident, the outcome of the risk assessment, any actions undertaken, the current residual risk (if any) and recommendations for further action. Where possible, recommendations should be provided to close an assessment report. Recommendations must be un-biased and take into account the following factors:

1. **Individual safety and wellbeing** – this includes 'duty of care' assistance for clients
2. **Protection of client/s personal information –** Only to be released per IPP guidelines
3. **Legislative guidance** – commonly criminal code and IPPs
4. **Departmental consequence** – Reputational damage through action/inaction
5. **Ongoing reporting to relevant stakeholders** – internal and external
6. **EAP and crisis management for staff involved in a critical incident**

2.65 Recommendations should assist in lowering a residual risk to an acceptable level, mitigating a risk entirely or recommending an action that may reduce the likelihood of a future event.