VAGO

Victorian Auditor-General's Office

Security of Government Buildings

May 2019

Independent assurance report to Parliament
2018–19: 21

VAGO

Victorian Auditor-General's Office

Security of Government Buildings

Independent assurance report to Parliament

Ordered to be published

VICTORIAN GOVERNMENT PRINTER
May 2019

PP 29, Session 2018–19

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 99% recycled content.

ISBN 978 1 925678 41 3

VAGO

Victorian Auditor-General's Office

The Hon Shaun Leane MLC
President
Legislative Council
Parliament House
Melbourne

The Hon Colin Brooks MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report *Security of Government Buildings*.

Yours faithfully

Andrew Greaves
Auditor-General

29 May 2019

Contents

Acronyms

CBD	central business district
CCTV	closed-circuit television
CPTED	Crime Prevention Through Environmental Design
DHHS	Department of Health and Human Services
DPC	Department of Premier and Cabinet
DJCS	Department of Justice and Community Safety
DJR	Department of Justice and Regulation
DTF	Department of Treasury and Finance
KPI	key performance indicator
ICT	information and communications technology
PSA	Physical Security Assessment
PSPF	*Protective Security Policy Framework*
RRA	Rapid Risk Assessment
SIRC	Security Incident Response Centre
SMAD	Security Management and Assurance Directorate
SPC	State Purchase Contract
SSP	Shared Service Provider
VAGO	Victorian Auditor-General's Office
VPDSF	*Victorian Protective Data Security Framework*
VPDSS	*Victorian Protective Data Security Standards*

Abbreviations

Accommodation Guidelines	*Victorian Office Accommodation Guidelines 2007*
Building standards	Victorian Government Office Building Standards
Security Management Framework	Whole of Victorian Government Security Management Framework: Government Office Accommodation Oct 2015

Audit overview

Security threats are an everyday risk to government agencies.

The risk comes from individuals or groups who, for a variety of reasons—some malicious—will seek to threaten staff, attack systems and processes, or damage or steal property. Unauthorised access to government buildings could put staff health and safety at risk and cause significant disruption to public sector services.

Government agencies keep their people, information and assets secure through protective security policies and practices. Physical security is one of three protective security domains, together with information and personnel security.

Physical security provides a first layer of defence to deter, detect, delay, and respond to threats and to recover from attacks after they occur.

Physical security measures are designed to provide and maintain a safe and secure environment for staff, clients, contracted service providers, and members of the public that use government facilities. These measures include policies and procedures, infrastructure and security design features.

Infrastructure-related measures include access control systems and closed-circuit television (CCTV).

An example of a policy is the clear desk policy that requires staff to clear all papers from their desks at the end of the day.

An example of a procedure is requiring visitors and contractors to sign in with personal identification at reception.

Effective governance should underpin all three domains of protective security. Strong security equally depends on government staff, contractors and visitors understanding the role they play in maintaining physical security, and continually observing security-related behaviours.

The Department of Treasury and Finance (DTF) is the lead agency responsible for coordinating office accommodation for its government clients across Victoria. The Shared Service Provider (SSP), DTF's internal business unit, provides office accommodation guidelines and works alongside government agencies to manage their office accommodation portfolio, including security services. Victorian government departments and selected agencies are required to buy security services through a State Purchase Contract (SPC). The SSP, however, only manages a small number of security contracts on behalf of its government clients.

We examined DTF in its role as the responsible department for coordinating government office accommodation across Victoria and managing the Security Services SPC.

We selected the Department of Health and Human Services (DHHS) and the Department of Justice and Community Safety (DJCS) as two examples of departments facing unique client challenges that may disproportionately affect staff and building safety. We tested the adequacy of physical security measures, access control and security culture at a selection of DHHS and DJCS occupied buildings.

Our overall objective for this audit was to assess whether government office accommodation is sufficiently secure to prevent unauthorised access and other criminal or antisocial behaviour.

Conclusion

The security infrastructure at the facilities we examined was adequate, but its effectiveness as a deterrent to unauthorised access was undermined by human error, enabled by a weak security culture. This weak security culture among government staff is a significant and present risk that must be urgently addressed.

At one site, we accessed discarded, sensitive information too easily. Unauthorised access to sensitive information has the potential to jeopardise the welfare and anonymity of already vulnerable government clients.

At present, there is no clear, strategic leader for policy, oversight and coordination of the three domains of protective security across government agencies. This precludes the better integration and coordination of protective security arrangements.

Findings

Physical security governance and statewide leadership

Victoria's current security governance arrangements are not fully effective. There is no statewide oversight or coordination of protective security, or any leadership that provides strategic direction on physical security policies and guidelines.

At the agency level, DJCS has made positive steps towards developing department-wide policies and procedures for security management. DHHS, however, has not developed its security policies and procedures, making it more vulnerable to unauthorised access.

Roles and responsibilities

Roles and responsibilities for security management between the SSP, the SSP's service delivery partner and the audited departments are not clear. This lack of clarity has caused delays in critical repairs, and inaction in establishing statewide security training.

Roles and responsibilities are further complicated in instances where the government leases accommodation from private landlords. The Assistant Treasurer signs the leases on behalf of the government; however, the agencies that occupy the office space are not privy to the terms and conditions of the lease even though the conditions impact them directly.

Strategic communications

The lack of regular strategic communication about security management between the SSP and the audited departments limits their ability to share good practice and collaborate on common security initiatives and issues. While the SSP regularly exchanges operational information with the audited agencies, the agencies have little ability to influence the management of security services as they do not have access to the terms and conditions in the security services contracts.

Security culture

The weak security culture in the audited departments leaves them vulnerable to breaches of security through human error. Statewide security assessments identified the most prevalent security issues as process, behaviour change, and cultural awareness. Despite the assessments, the audited departments have not prioritised security training for staff, though DJCS is in the early stages of developing staff training as part of its overall protective security approach. To date, DHHS has not developed any staff security training.

Risk assessment

Ongoing and comprehensive risk assessment underpins effective security planning. Following the raised National Terrorism Threat Level in September 2014, DTF coordinated a one-off Rapid Risk Assessment (RRA) program across all the government buildings it manages. However, the program had limited effectiveness for several reasons:

- The RRA audited current security measures rather than identifying and quantifying the security risks.
- DTF did not clearly define the objective and outcome of the RRA process, which resulted in a deficient process for implementing recommendations.
- Individual departments were responsible for determining what, when, and to what extent they implemented the recommended actions, limiting the overall effectiveness of the RRA and the number of recommendations implemented.

The audited departments have not undertaken risk assessments outside of the RRA process. Consequentially, security planning is not adequately informed by, and responding to, the level of risk.

Managing physical security

Adequacy of physical security measures

We tested the physical security at selected DHHS and DJCS offices to assess the adequacy of their security measures. While we found some examples of staff questioning testers and verifying identification, we bypassed physical security measures and accessed the office accommodation at the tested sites.

Staff at these offices did not fully understand their role in maintaining physical security and in some instances did not comply with established processes. We also identified serious breaches of physical and information security.

Accommodation planning and management

There is little assurance that the state and the audited departments use appropriate accommodation planning and management to achieve the best security outcomes. The current statewide guidelines for government office accommodation are outdated and do not reflect better practice.

DJCS has developed its own accommodation planning guidelines and design standards for its regional offices, which creates design efficiency and ensures a consistent minimum approach to physical security. In contrast, there is limited consistent consideration of security in DHHS's accommodation planning.

Base building refers to the shared areas of a multi-tenant building; for example, the lobby, loading dock, car park, lift well, or stairwell.

When leasing accommodation from private landlords, government often has limited input into the base building design and security measures. There is no systematic arrangement for the state or the government agencies under the lease to have visibility of base building incidents and risks. While risk can never be eliminated entirely, DTF needs to take measures to mitigate it.

Security services

Currently, security services such as guarding, mail scanning, and concierge services are limited in their effectiveness to create a safe and secure working environment. Weak governance arrangements have contributed to this, as have physical security measures that are implemented without strategic security planning or proper risk assessment.

Currently, the state has limited visibility and control over how security services are managed. The SSP manages 331 government buildings in total, but only 38 use the security services under the SPC. There is no SPC for security systems, such as alarm monitoring and maintenance, which further limits statewide control of security management.

Departments do not advise the SSP when they procure security services independently, so the SSP does not know how often this occurs or what the cost of those contracts are.

The SSP relies on complaints and exception-based reporting to measure the performance of security service providers. The SSP does not conduct regular audits of the security services, which limits its ability to address security concerns in a timely and risk-based manner.

Security incidents

The ability to respond to security incidents in a timely manner is critical to staff safety and is better practice in managing security risks. Furthermore, a risk-based approach to incident investigation is an important step towards identifying vulnerabilities and improving staff culture for the future.

The government does not have an accurate understanding of the nature or number of physical, or protective, security incidents in government-occupied buildings. This is because the SSP and DJCS do not yet have mature incident reporting and monitoring procedures or systems, while DHHS does not have an integrated incident reporting system. Better processes are needed for incident reporting, monitoring and evaluation, including risk-based incident classification.

The current approach to incident reporting, monitoring and evaluation is a missed opportunity to learn from previous incidents to modify and improve security.

Recommendations

We recommend that the Department of Treasury and Finance:

1. in collaboration with key security agencies such as Department of Premier and Cabinet and the Department of Justice and Community Safety, develop a statewide principle-based physical security policy, with clear accountabilities for government agencies (see Section 2.2)
2. finalise the office accommodation guideline update, including better practice for physical security design and controls (see Section 3.3)
3. improve statewide incident reporting for physical security, by:
   - sharing incident reports and the incident dashboard with affected departments in a timely manner (see Section 3.5)
   - developing mechanisms for incident reporting at sites without guards and at privately leased accommodation (see Sections 3.3 and 3.4)
   - developing security incident classification and risk ratings to improve incident reporting and evaluation processes (see Section 3.5)
4. explore options for the creation of a State Purchase Contract for security monitoring and maintenance systems (see Section 3.4)
5. develop key performance indicators for the security management element of its 'real estate and facilities management' service contract (see Section 3.4)
6. improve strategic communication with its client government agencies by regularly sharing emerging trends, risks and better practice (see Section 2.2)
7. provide accommodation terms and conditions in the lease to the government agency tenant to facilitate security management (see Sections 2.2 and 3.3)
8. provide government agencies with the provisions in the Security Services State Purchase Contract and associated contracts that impact on their management of office accommodation (see Section 3.4).

We recommend that the Department of Health and Human Services and the Department of Justice and Community Safety:

9. promote a strong security culture and good governance, by developing and finalising:
   - an agency-wide physical security policy in line with best practice principles (see Section 2.2)
   - physical security incident reporting, investigation and evaluation processes (see Section 3.5)
   - physical security training and monitoring completion rates (see Section 2.2)
   - implement and enforce clean desk and clear screen policies, including periodic audits or checks against staff compliance (see Section 3.2)

10. undertake regular physical security planning and risk assessment (see Section 2.3).

We recommend that the Department of Health and Human Services:

11. develop design standards for accommodation planning and office refurbishments at client facing locations, incorporating minimum security measures and controls (see Section 3.3)
12. develop a governance structure for security management, including clear accountability and adequate executive oversight (see Section 2.2).

Responses to recommendations

We have consulted with DTF, DHHS and DJCS and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report to those agencies and asked for their submissions or comments. We also provided a copy of the report to the Department of Premier and Cabinet (DPC).

The following is a summary of those responses. The full responses are included in Appendix A.

The three audited departments accepted all recommendations. DPC, while not an audited agency, accepted recommendation one and will work with key agencies to implement it.

1
Audit context

Government agencies face a real and credible threat to their physical security and the safety of their client-facing staff. Unauthorised access to government buildings could cause significant disruption to public sector services while antisocial behaviour from government clients puts staff health and safety at risk.

Prevention and minimisation of security incidents is everyone's responsibility. It requires government agencies to have strong physical security measures, including physical controls, to secure the perimeter and control access to buildings. Strong security equally depends on government staff, contractors and visitors occupying the building to understand the role they play in maintaining physical security, and continually observing security-related behaviours.

A strong security culture can significantly decrease the opportunity for wrongdoing and the risk to an organisation, its people, assets or information. According to the Commonwealth's 2018 *Protective Security Policy Framework* (PSPF), such a culture is one where:

- security is prioritised and promoted across the organisation
- security is built into the organisation's business operations
- staff understand the security risks that relate to them
- security awareness training is effective in educating staff about their security obligations and the organisation's policies and procedures
- security incidents are reported and investigated.

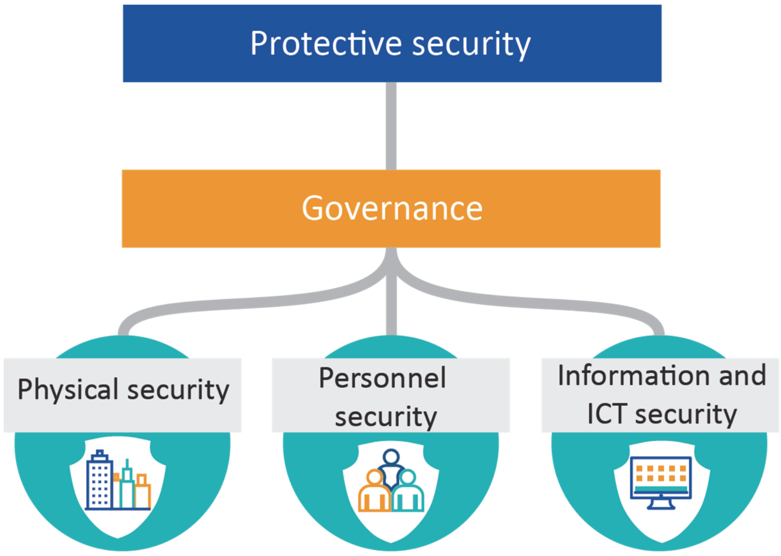
Protective security

Protective security is the term used to refer to the collective policies and practices used to keep government's people, information and assets secure. As shown in Figure 1A, the PSPF outlines three protective security domains:

- physical security
- personnel security
- information, and information and communications technology (ICT) security.

Effective governance arrangements should underpin all three domains.

Figure 1A
Protective security



Source: VAGO.

Physical security

In this audit, we examined physical security, which aims to provide and maintain a safe and secure working environment for staff, clients, contracted service providers, and members of the public. Physical security measures are often the first line of defence in a layered approach to protective security.

In its *Victorian Office Accommodation Guidelines 2007* (Accommodation Guidelines), DTF recommends using Crime Prevention Through Environmental Design (CPTED) principles. CPTED focuses on designing the physical environment to have:

- natural access control—to restrict criminal intrusion
- natural surveillance—to keep potential offenders and intruders under observation
- territorial reinforcement—to delineate private spaces from semi-public and public spaces, while creating a sense of ownership so that intruders stand out.

The CPTED principles promote layers of defence to 'Deter, Detect, Delay, Respond and Recover' from threats or intruders, or slow the progress of security incidents, preventing a larger or more serious breach. Figure 1B shows how the PSPF's 'Deter, Detect, Delay, Respond and Recover' approach can be used to create layers of defence.

Figure 1B
Deter, Detect, Delay, Respond and Recover approach

Deter	Measures implemented that adversaries perceive as too difficult or needing special tools and training to defeat. For example: barriers and access control, guards, public visibility.
Detect	Measures implemented to determine if an unauthorised action is occurring or has occurred. For example: security guards, CCTV, alarms, public visibility.
Delay	Measures implemented to impede an adversary or slow the progress of a detrimental event to allow a response before agency information or assets are compromised. For example: barrier and access controls, swipe cards.
Respond	Measures taken once an agency is aware of an attack or event, to prevent, resist or mitigate the attack or event. For example: enact local procedures, alert authorities and law enforcement.
Recover	Measures taken to restore operations to normal (if possible) following an incident. For example: enactment of business continuity and/or recovery plans.

Source: VAGO, based on the PSPF.

Policy, frameworks and guidelines

Victorian Security Management Framework

DTF’s Whole of Victorian Government Security Management Framework: Government Office Accommodation Oct 2015 (the Security Management Framework) is a guide for office accommodation building security. It is not mandatory but informs departments and agencies of the minimum expected standards across government. The Security Management Framework reinforces the ‘Deter, Detect, Delay, Respond, and Recover’ approach and provides some specific guidelines for security; for example, in relation to building location, access and multi-tenancy arrangements.

The framework establishes the following security management elements:

- the decision framework—applicable policies, standards and guidelines
- assessments—the program of assessments known as the Rapid Risk Assessments, which encourages the ongoing evaluation of risk
- emergent actions—actions resulting from the assessments, which are implemented and fed into the accommodation planning strategy.

A threat level of PROBABLE means security agencies have credible intelligence to indicate that individuals or groups have the intent and capability to conduct a terrorist attack in Australia.

The Security Management Framework was developed following the Commonwealth Government raising Australia's National Terrorism Threat Level to 'high' which is equivalent to the current 'PROBABLE' rating in the new system.

Victorian Government Office Accommodation Guidelines

The Victorian Government owns and occupies a significant amount of office accommodation across Victoria. As of November 2018, DTF was responsible for managing 331 government leased and owned buildings.

DTF's Accommodation Guidelines are used by government departments and agencies to establish their requirements for accommodation planning, leasing, fit-out and management. These Accommodation Guidelines, supported by the *Victorian Government Office Building Standards* (Building Standards), are a tool to assist departments and agencies in procuring the most appropriate office accommodation to meet the needs of government. They create consistent standards and benchmarks across government and should form the basis of government office accommodation planning and design.

The Accommodation Guidelines and Building Standards contain advice and requirements for security, such as:

- applying the CPTED principles in the design of office accommodation
- complying with Australian Security Intelligence Organisation office building specifications
- requiring minimum controls to secure the office—such as CCTV and intrusion detection systems.

A **control** in the context of security management is a measure used to protect official information from compromise of confidentiality, or mitigate an identified threat to an agency's people, information or assets.

The Accommodation Guidelines do not apply to operational accommodation areas. Examples of operational areas within DHHS and DJCS are prisons, interview and program rooms, and transaction counters.

Victorian Protective Data Security Framework

The Office of the Victorian Information Commissioner's *Victorian Protective Data Security Framework* (VPDSF) and *Victorian Protective Data Security Standards* (VPDSS) establish 18 high-level mandatory requirements, containing 117 elements. The VPDSS creates obligations for every Victorian government agency relating to:

- security governance
- information security
- personnel security
- ICT security
- physical security
- assurance.

The VPDSF came into effect in July 2016. All government agencies attested to their compliance with it in August 2018 and are required to do so every two years. The VPDSF covers physical security as it relates to information protection and is not intended to be an outright guide for physical security.

Commonwealth Protective Security Policy Framework

The PSPF was first developed by the Commonwealth Attorney-General in 2012 and was most recently updated in October 2018. The PSPF is the Commonwealth Government's protective security policy to assist Commonwealth entities to protect their people, information and assets. It provides guidance and establishes core requirements for Commonwealth agencies across the domains of protective security governance, personnel security, physical security, and information and ICT security.

The PSPF and its requirements represent better practice for state government agencies. However, it is not mandatory in Victoria, so government agencies have no obligation to implement it. The framework applies a security risk management approach, which focuses on fostering a positive culture of security within and across government.

There are two PSPF standards for the management of physical security. *PHYSEC15—Physical security for entity resources* requires agencies to implement physical security measures that minimise the risk of harm to people, or the risk of information and assets being destroyed or used without authorisation.

The PHYSEC16—Entity facilities outlines the need for protective security to be integrated into the planning, selecting, designing, and modifying of facilities (such as office accommodation). This includes zoning office areas and restricting access based on the need to protect confidential information or valuable assets. The PSPF defines the following security zones:

- zone one—unsecured and public access areas; for example, a lobby or reception
- zone two—low security areas with some access controls for visitors; for example, general staff office areas
- zone three—restricted staff access areas and visitor access on an as needs basis, supervised by staff
- zones four and five—restricted areas with high security needs and strictly regulated staff and visitor access.

Security Services State Purchase Contract

Under section 16(1) of the *Public Administration Act 2004*, Victorian government departments and selected agencies are required to use the SPC for the provision of security services.

The Security Services SPC offers:

- static guarding, including:
  - concierge/reception duties
  - producing and issuing passes to personnel
  - searching personnel and their belongings
  - recording visitor entry and departure times
  - onsite and offsite control room operations
  - responding to routine and emergency incidents
- patrolling sites
- mail and parcel scanning
- alarm response
- other ad hoc requirements such as static guarding for special events.

The Security Services SPC was first established in July 2013 and the current SPC is the second panel in operation. Managed by DTF, the SPC is a closed panel arrangement with five suppliers. Total expenditure under the former SPC during 2016–17 was $46.6 million. This decreased to $38.5 million in 2017–18.

The new SPC commenced on 1 February 2018 for a period of three years, with extensions available. The SSP currently manages three contracts for government security services. Security is provided to 38 government buildings under the Security Services SPC, which makes up only 11.5 per cent of the total 331 buildings that the SSP manages on behalf of the state.

1.1 Roles and responsibilities

DTF is the lead agency responsible for coordinating government office accommodation for its government clients across Victoria. It provides guidelines and works with departments and agencies to manage all aspects of their office accommodation portfolio, including real estate, facilities management and security risks. Within DTF, the SSP is the business group responsible for providing these services.

In addition, DTF contracted a private organisation to be its service delivery partner for the provision of real estate and facilities management services, which commenced on December 2017. The service delivery partner manages over 300 government owned and leased office properties across Victoria, including security management services. The total estimated value of this contract is $41.3 million over 5.5 years.

Under the Victorian *Occupational Health and Safety Act 2004*, the accountable officer—the department secretary or agency leader—has a duty of care to create a safe and secure environment for ministers, employees, contract service providers, tenants and visitors.

1.2 Why this audit is important

Unauthorised access to government buildings could put staff health and safety at risk and cause significant disruption to public sector services. Therefore, it is critical that:

- DTF provides departments and agencies with comprehensive and up-to-date guidance on how to best mitigate building security risks
- departments and agencies apply this guidance, to meet the appropriate level of security.

Statewide government building security has not been examined in detail by VAGO, or other external agencies.

1.3 What this audit examined and how

The objective of this audit was to determine whether Victorian Government office accommodation is sufficiently secure to prevent unauthorised access and other criminal or antisocial behaviour that may threaten the safety of staff, visitors and members of the public. The audit examined physical security as it relates to protective security and did not examine emergency management or counter-terrorism procedures.

We examined DTF in its role as the responsible department for coordinating government office accommodation across the central business district (CBD), and metropolitan and regional areas, and managing the Security Services SPC.

We selected DHHS and DJCS as two examples of departments facing unique client challenges that may disproportionately affect staff and building safety. We assessed whether these departments have effective governance and risk management arrangements, and sufficient controls to prevent unauthorised access and antisocial behaviour. This included testing controls and security at selected CBD, metro and regional DHHS and DJCS office locations.

To do this we:

- interviewed DTF, DHHS and DJCS staff
- observed security controls at selected sites
- reviewed key documentation relating to policies, guidelines, risk management, incident reporting and evaluation
- engaged a specialist security consultant to undertake risk assessments as well as physical security testing of selected sites.

We conducted our audit in accordance with section 15 of the *Audit Act 1994* and ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements related to assurance engagements. The cost of this audit was $327 000.

1.4 Report structure

The remainder of the report is structured as follows:

- Part 2 examines governance arrangements for effective physical security
- Part 3 examines the management of physical security.

2 Physical security governance

Security culture and governance underpin effective security management. Without a strong security culture, security measures and controls are vulnerable to human error. Even the best access control system will fail if staff are careless with their access cards or lend them to others. A consistent security culture across government requires strong leadership, an enforceable accountability framework and a principle-based policy.

Across the state, government agencies can develop governance structures to best suit their operational needs. The structures should be supported by a strong security culture. Agencies should promote security across the organisation, embed security in their day-to-day operations, monitor and investigate security incidents, and educate staff about security risks, obligations, policies and procedures.

In this Part of the report, we examine whether departments have effective physical security governance arrangements, management structures and a strong security culture.

2.1 Conclusion

Currently, security governance at the state and department levels is not effectively preventing unauthorised access to government accommodation. The SSP, as a service provider, is responsible for the security operations of its clients, but is not a statewide policy lead for physical security. As such, there is no system leader to provide strategic oversight and direction. Roles and responsibilities for security management are not clear between the SSP and departments, which at times has resulted in confusion, delays, and inaction when trying to respond to security risks.

The SSP and the audited departments do not have an ongoing cycle of risk assessment. Assessments conducted to date are audits of security measures rather than assessments of the level of security risk government departments face. Current security planning within the audited departments is subsequently limited, as planning should be based on a comprehensive understanding of risk.

In the absence of statewide leadership, we found two different approaches to physical security at the department level. DJCS has taken a more proactive approach and is in the process of developing department-wide policies and procedures for security management. DHHS does not have department-wide security policies and procedures, exposing it to higher risks.

Significantly, we observed a weak security culture at the selected DHHS and DJCS sites that leaves their office accommodation, and the people and information within it, vulnerable to breaches of security through human error.

2.2 Governance

DHHS and DJCS face unique client challenges that may compromise safety, and they are both acutely aware of the need for physical security to protect their staff, information and assets. Despite their awareness, we found that DHHS and DJCS did not have, or had not finished developing and implementing, effective governance arrangements to best support physical security.

DHHS does not have a centralised structure for the oversight of policies to support physical security governance. While divisions have some operational security procedures, these lack consistency. In the absence of strong leadership from the SSP, DHHS has not yet sought to develop its own physical security policies, training, or incident reporting procedures.

While still in the formative stages, DJCS is setting up a good governance framework for physical security, as part of its approach to protective security. DJCS's dedicated Security Management and Assurance Directorate (SMAD) is focused on developing a strong security culture within the department.

Policies and procedures

Victoria does not have a whole-of-government security policy that is principle-based and includes all stages of security management. DTF's Security Management Framework limits its scope to accommodation planning. It is not mandatory or enforceable but contains the minimum expected accommodation security standards across government.

However, departments advise that some of the specific standards it sets out are not practical in their operating environment and are difficult to comply with, which limits the value of the Security Management Framework. For example, the Security Management Framework suggests that government office accommodation should not be co-located with commercial businesses (such as restaurants, cafes or retail shops) and that shared tenancy arrangements with non-government organisations is not desirable. We also found that the framework is not well known or used at the two departments we audited.

A principle-based policy provides high-level outcomes and objectives. Departments and agencies can achieve the outcomes in a way that suits their organisation and operating environment.

Without an enforceable principle-based policy, departments may create inconsistent practices or seek out alternative standards, such as the PSPF. It could also lead departments to operate without any policy direction, as we found with DHHS in this audit.

DHHS and DJCS do not have completed, endorsed physical security policies, but they do have some current operating procedures. The departments are at varying stages of progressing their physical security policies.

Department of Health and Human Services

DHHS does not have a physical security policy and instead relies on DTF for policy guidance. However, DTF does not have an enforceable security management policy.

DHHS has recently identified the need for a policy through the VPDSS attestation process. DHHS's physical security policy is due to be completed by December 2019. In parallel, the DHHS accommodation management team is in the early stages of scoping a Security Risk Management Framework project. One output of this project will be the development of a security policy that aims to 'ensure staff behaviours and all client interactions and responses are within clearly established best practice guidelines'. To date, the project has not been approved and there are no dates established for key deliverables.

Department of Justice and Community Safety

DJCS is currently drafting its overarching Security Policy Framework and an associated Security Manual. The framework will cover all the protective security domains.

The intention is for the manual to support existing processes and procedures, to be a tool for staff to familiarise themselves with the minimum-security requirements and to embed a security culture across DJCS. The manual is designed to closely align with the VPDSS and the PSPF. The planned sections of the manual are:

- security governance
- information security
- personnel security
- ICT security
- physical security
- security assurance.

The physical security section is still to be drafted, however other sections such as personnel security are well progressed. DJCS states that once written, its physical security chapter will align closely with the Commonwealth PSPF's *PHYSEC16—Entity facilities.*

Roles and responsibilities

Statewide

The roles and responsibilities of the SSP and the government agencies they represent are not clearly defined or agreed.

This is further complicated when trying to distinguish between the responsibilities of the SSP, the SSP's service delivery provider, government agencies, the security providers and, if located in privately owned office accommodation, the building landlord.

The confusion is further exacerbated by several other factors, such as:

- the lack of regular strategic communication and information-sharing forums between the SSP and government agencies
- government agencies not having access to the terms of accommodation leases, as discussed in Figure 2A
- the lack of a single agency responsible for a statewide physical or protective security policy.

Figure 2A
Case study: Replacement of DJCS's uninterrupted power supply

An uninterrupted power supply (UPS) is an electrical apparatus that provides emergency power when the input power source or mains power fails. The former Department of Justice and Regulation (DJR) became aware that its UPS system required replacement in June 2016.

When the Assistant Treasurer enters into leases with private landlords on behalf of Victorian government agencies, departments who occupy the office accommodation are not a party to the lease and not privy to its terms, which outlines roles and responsibilities. As a result, DJR was unclear about who was responsible for the UPS replacement.

After three months, the UPS issue was still not rectified. The department considered the replacement to be urgent and delays increased its level of risk.

Following the final resolution of this issue, DJR made efforts to clarify and document whether the SSP or DJR was responsible for building service functions and assets. However, we found that there is still confusion over responsibility for the UPS.

Source: VAGO, based on information provided by DJCS.

Department of Health and Human Services

DHHS does not have an effective or clear structure for physical security governance, policy or strategic planning. Responsibility for operational management and accommodation planning is shared between the central Accommodation Management unit of DHHS's Procurement, Contract Management and Business Services Branch, and the DHHS operational divisions.

On a day-to-day basis, the central accommodation team is responsible for elements such as accommodation planning, risk assessments, implementing security measures and managing the relationship with the SSP. Some operational responsibility, such as for DHHS-owned CCTV, duress alarms and incident response procedures, is devolved to each DHHS Division's Business Services Manager.

While the central accommodation services team has responsibility for physical security governance, they state that their small staff responsible for security, the full-time equivalent of 0.4, has resulted in the prioritisation of other elements of office accommodation and security. As such, DHHS does not have a consistent or organisation-wide approach to physical security policies, training, incident reporting or investigation.

Executive oversight for physical security is ad hoc. Leadership is briefed on issues when and as required, rather than through regular updates or via oversight by a security committee. If DHHS implements its Security Risk Management Framework project, it will include a governance structure with senior DHHS representation to provide whole-of-portfolio oversight. It is unclear whether such a structure would be specific to the project or would include the oversight of security and accommodation planning more broadly, and be ongoing.

DHHS's governance structure does not align with the PSPF's recommended structure, which is reasonable, as departments should be encouraged to develop a structure that is effective for them. However, DHHS's current gaps in security governance have resulted in limited executive oversight and no physical (or protective) security policy.

Department of Justice and Community Safety

DJCS's governance structure positions physical security as one element of its protective security policies and procedures. There is a clear delineation between DJCS's governance and its operational arms for physical security. SMAD is responsible for protective security at a strategic and policy level, creating consistency and standards across all the DJCS regions. SMAD is responsible for protective security policies, procedures, training, cultural awareness, incident reporting and management. The Assets, Infrastructure and Major Projects Branch is responsible for the day-to-day management of DJCS's office accommodation and is the key point of contact with the SSP.

DJCS's governance structure broadly aligns with the PSPF's suggested security governance structure. There is adequate executive oversight of physical security (and protective security more broadly) through DJCS's security committees. The department's Security Program Board and its Emergency Management Committee support the work of the Security Executive Committee to implement DJCS's security and emergency management frameworks. These committees have a broad membership from across the department, its regions and some portfolio entities. The Security Executive Committee reports to the DJCS's Board of Management.

Information sharing and better practice

There is regular communication between the SSP and government agencies on operational matters, as well as monthly executive meetings and fortnightly operational meetings. However, collaboration and communication on strategic direction or projects—such as whole of Victorian Government training or sharing of better practice—is limited.

The SSP held a security forum in November 2017 for its key contacts within the government agencies they represent. The forum's purpose was to discuss topical issues, share problems and collaborate on solutions. The forum included discussion about whole of Victorian Government issues such as risk assessments, security training, alarm centralisation, incident reporting, and guarding services. While DJCS and DHHS had positive feedback about the forum, the forum has not been repeated since, despite the intention of it being ongoing.

There is an opportunity to improve communication among physical security stakeholders and formalise communication channels. Continuation of the security forum, or a community of practice, would provide government agencies with the opportunity to promote and seek advice on security practices, policies and procedures. During our audit, we found DHHS and DJCS both had elements of better practice that would be beneficial to share with other government agencies.

Security training

Baseline security training for staff is important in establishing a positive security culture. Training supports the implementation of security controls and policies. It communicates the expected behaviours and responsibilities and educates staff on the agency's policies and procedures. Staff in senior or specialised roles may require specific or more detailed training.

The need for security awareness training was evident from the results of the RRA. The RRA was a one-off security assessment program, discussed in more detail in Section 2.3 of this report. Training and security culture were part of the fourth priority category of RRA recommendations, which included 'process changes, awareness, behaviours, minor works'. Fourth priority recommendations made up 63 per cent of all recommendations statewide. However, as at July 2018, departments had only implemented 28 per cent of priority four recommendations.

As yet, neither of the audited agencies have established baseline or department-wide training for physical or protective security. A weak security culture, and lack of regular training, leaves departments vulnerable to breaches of security through human error.

Department of Treasury and Finance

DTF has drafted content for a physical security online training module and has consulted with departments on the draft. The draft training is principle-based and informs participants on good security behaviours such as a clear desk policy, staff security pass handling and procedures, and common physical security measures.

While taking the lead for the training is a positive step, we found that there is confusion between DTF and the departments about the commitment to and responsibility for this training. In particular, there was a lack of clarity around whether developing the online training product will be led by DTF or whether the draft content should be used by departments as a base and further revised to suit the needs and operating environment of each department. Development of the training has not progressed since August 2017, highlighting the need for a lead security agency to champion improvements and better practice.

Department of Justice and Community Safety

DJCS does not have department-wide security training but does have training specifically for its client-facing staff. DJCS also undertakes emergency management and crisis training exercises and has implemented security awareness initiatives such as displaying posters and publishing content in the internal DJCS newsletter.

Through SMAD's Security Management Framework and associated communications plan, SMAD has documented its intent to develop mandatory protective security awareness training as well as induction training for new employees of DJCS. To date, SMAD has circulated several protective security fact sheets.

Department of Health and Human Services

DHHS does not have department-wide physical security training, but it identified this need in its response to the VPDSS in 2018. The DHHS divisions have regular training for some operational aspects of security, such as incident response and duress alarms, but do not have any principle-based training.

2.3 Risk assessment

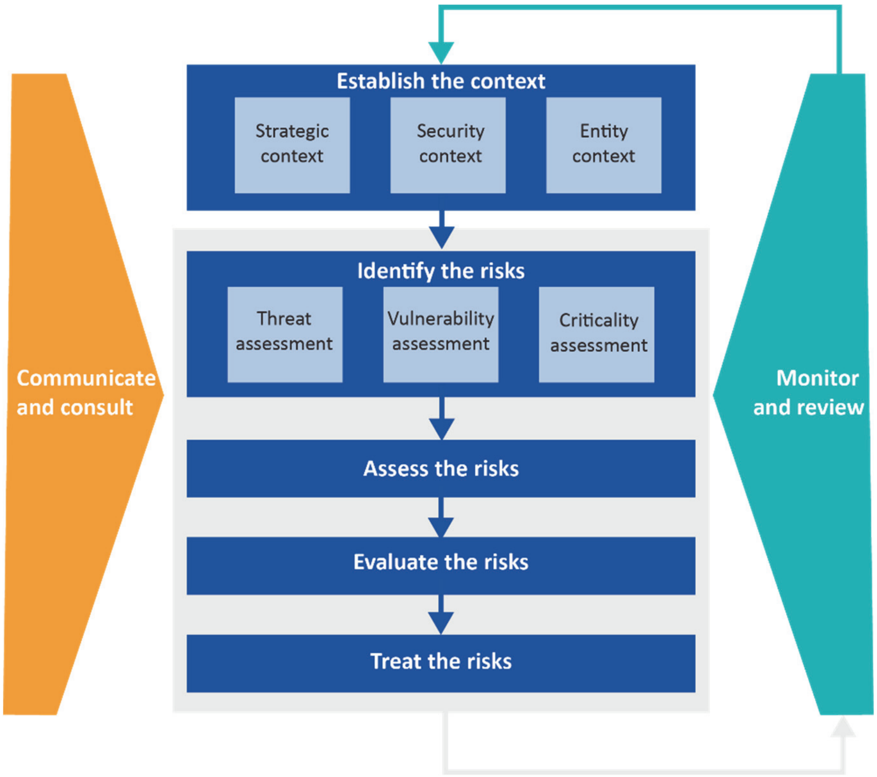
A security risk, as defined by the PSPF, is something that could result in harm to staff, or the compromise, loss, unavailability of or damage to assets.

Regular and comprehensive risk assessment is an integral part of an organisation's security management.

Risk assessment involves identifying the criticality of an organisation's resources, the likelihood and consequences of threats, and the degree of susceptibility and resilience to threats. The outcomes from risk assessments should inform an organisation's security planning decisions, including whether additional protective security controls are required. Government agencies need to consider what needs protecting, what the threat is and how assets will be protected.

Figure 2B outlines the PSPF's recommended framework for Commonwealth government agencies to use when assessing protective security risks.

Figure 2B
PSPF risk assessment framework



Source: VAGO, based on the PSPF.

The audited departments do not undertake regular and comprehensive risk assessment for physical security. They were involved in a one-off risk assessment program known as the Rapid Risk Assessment (RRA).

Rapid Risk Assessment

In September 2014, following the raised National Terrorism Threat Level, DTF coordinated security assessments of government-owned and leased buildings, which later became known as the RRA. DTF worked closely with Victoria Police and prioritised the assessment of CBD departmental office accommodation (including ministerial offices), courts and critical infrastructure. The RRA was gradually rolled out to other government buildings in regional areas and concluded in December 2017.

Conducting the RRA was an appropriate and proactive response because, at the time, it was considered likely that the threat level would remain at ‘high’ (equivalent to the current ‘PROBABLE’ classification) for the foreseeable future. These assessments resulted in hundreds of recommended security improvements for government accommodation. However, the program fell short in what it could have achieved due to a lack of overall governance and a clear project scope.

The RRA assessors documented the physical security measures at each site, as Figure 2C outlines.

Figure 2C
Security assessments included in a typical RRA

An RRA assessed whether the following security measures were in place:

- physical controls to prevent unauthorised or forced access, such as security bollards, barriers, fences, gates, lifts, doors
- access and exit procedures and systems for staff, contractors and visitors, such as the use of identification cards and procedures for lost cards
- mail and parcel delivery and scanning procedures
- security monitoring technologies used, such as CCTV and relevant response procedures
- designated staff or security guards on site to prevent and react to security incidents, and relevant procedures to respond to various incidents
- electronic duress alarms on site and relevant response procedures.

In addition, an RRA also evaluated whether the layout of the office and surrounding area was consistent with good CPTED principles. For example, whether a security officer could obtain a clear line of sight to the public waiting area from where they are positioned.

Source: VAGO, based on RRA reports.

In practice, the RRAs were an audit of the security measures in place, in response to the raised security alert, and the urgent need to identify and recommend improvements to the physical security measures at government office accommodation. It was not intended to be a security risk assessment as defined in the PSPF or any other risk assessment standard such as the ISO 31000—*Risk Management*. The RRAs prioritised assessment of CBD buildings, but did not assess the criticality of an organisation's resources, the site-specific risk profile or vulnerabilities.

While called a risk assessment, some RRAs did not conclude with a risk rating. We reviewed 29 RRA reports for a selection of DHHS and DJCS locations. Within our sample, five security consultants were engaged. Of the 29 reports, only 16—all written by the same security consultant—included a statement about the level of risk.

DTF acknowledges that the RRA did not start with a clear project scope. Without a consistent report template and assessment criteria, the quality of the RRAs varied considerably. This was further complicated by the fact that several different security consultants were engaged, who used varying approaches to their assessment and a different style and reporting format. While similar security measures were covered, they differed in the level of detail assessed.

Although DTF attempted to standardise the RRA methodology during the rollout, the inconsistency in methodology resulted in recommendations of varying quality. In some cases, recommendations were considered disproportionate to the risks identified. Despite becoming aware of this issue, DTF did not evaluate or moderate the appropriateness of these recommendations. It was at the discretion of the departments to accept and implement the recommendations.

Physical security assessments

Recognising that risk assessment is a continuous process, the SSP has commenced planning for a new Physical Security Assessment (PSA) to replace the RRA. To date, the SSP has not formally launched the PSA but has undertaken some assessments upon request. The objective of the PSA is to assist government agencies to 'achieve a level of physical security infrastructure and procedures that are sufficient to provide for the safety and security of site users in the context of the current National Terrorism Threat Level and the realistic assessed security risk to each site/building'.

By providing a standardised PSA template to guide the assessment, the SSP expects the assessment and any resulting recommendations will be more consistent than the RRA program.

We assessed two of the PSAs conducted to date and note that while most of the security measures assessed are similar to the RRA, some improvements have been made. The PSA has clearer scope requirements than the RRA. In comparison, the security measures are now more clearly defined in the template. For example, instead of the simple reference to 'security monitoring including CCTV' in the RRA, the PSA requires specific detail about the CCTV on site, such as its storage capacity and basic specifications.

The PSA also includes new elements that were not included in the RRA scope; for example, whether each site has an emergency plan (including security provisions) and whether there is a lockdown procedure.

Although the PSA user guide states that it aims to provide a realistic assessment of the security risk to each building, the template provides little guidance on how this needs to be done. The template's only reference to site-specific risk assessment is to ask the assessor to provide 'any other relevant information with respect to site security situation, threats or risks'. In the examples we reviewed, this field was recorded as 'N/A'—not applicable.

The SSP advises that it no longer uses the word 'risk' in the assessment as this triggers a number of technical assurances and standards, and significantly increases the cost of the assessments. While this may be a practical response, without a comprehensive risk assessment, security planning has limited effectiveness. We discuss this further in Part 3.

Implementing the RRA and PSA recommendations

By the end of July 2018, the RRA program had generated 2 152 recommendations from the assessment of 280 sites. The SSP categorised these recommendations into four types, where type one was the highest priority for implementation and type four was the lowest. The SSP advised that the level of urgency was determined by Victoria Police as follows:

- type one—guards/guarding services
- type two—access systems and controls
- type three—CCTV and alarms
- type four—all remaining recommendations, but particularly process and behaviour change, cultural awareness, and minor site-specific works.

Recommendations were not mandatory. There was no statewide budget dedicated to the implementation of RRA recommendations or central oversight for quality or timeliness of the progress. Individual agencies were responsible for deciding whether, to what extent and when to implement the recommendations. SSP managed physical works through its contractors and reported the status of progress once the agency approved and funded the works.

Figure 2D shows the overall progress against implementing these recommendations as at July 2018.

Figure 2D
Departmental implementation of RRA and PSA recommendations as at July 2018

Urgency category	Total number of recommendations	Per cent completed	Per cent in progress	Per cent still to commence	Per cent suspended
Type one	60	68%	5%	7%	20%
Type two	247	36%	11%	31%	22%
Type three	483	42%	5%	39%	13%
Type four	1 362	28%	7%	45%	20%
All recommendations	2 152	33%	7%	41%	19%

Note: Figures have been rounded.
Source: VAGO, based on documentation provided by DTF.

The category of 'suspended' reflects works that departments did not accept or implement. Specific reasons for suspensions were not documented, however the audited agencies have stated that recommendations were suspended:

- if they were considered disproportionate to the level of risk
- because of budgetary constraints
- because the agency intended to relocate in the immediate future
- because the recommended action was outside of the agency's authority.

In certain cases, other works or projects addressed the intention of the recommendation, and it was marked as suspended.

Departments implemented type one recommendations as their first priority; 68 per cent were implemented, which was the highest rate of completion. While type four actions made up most recommendations (63 per cent), the completion rate was the lowest at 28 per cent.

DJCS and DHHS took different approaches to implementing recommended actions.

Department of Justice and Community Safety

DJCS's approach to addressing RRA recommendations reflected that security management requires the support of department-wide policies and procedures and that security is everyone's business.

As of July 2018, DJCS received a total of 383 recommended actions from both the RRAs and PSAs. Type four actions made up 57 per cent of all recommendations.

Figure 2E
Progress of security improvements at DJCS as at July 2018

DJCS recommendation	Total number of recommendations	Per cent completed
Type one	12	83%
Type two	49	29%
Type three	104	42%
Type four	218	32%
All recommendations	383	36%

Note: Figures have been rounded.
Source: VAGO, based on documentation provided by DTF.

In its implementation, DJCS improved physical controls and developed procedures and processes to improve security culture. For example, it:

- developed safety standard operating procedures for mail handling, duress testing, and the use of interview rooms
- rolled out training at its regional offices relating to managing drug and alcohol affected, mentally ill or aggressive clients
- developed an online training program that set out the responsibilities and attributes of the safety systems in regional sites.

Currently, DJCS is embedding security training to implement type four recommendations. Security posters are prominently placed in corridors and work stations. These include advice to staff on:

- the security benefits of a clear desk policy
- removing their lanyards once in public to reduce the potential of being identified as government staff or as a target for tailgating.

DJCS's overall approach to implementing recommendations reflects better practice. Its initiatives, although still in development, should improve security management practices within DJCS moving forward.

Department of Health and Human Services

As of July 2018, DHHS received 509 recommended actions, of which 323, or 63 per cent, were type four. DHHS implemented improvements in access and site-specific building works. DHHS decided to take a phased approach to implementing recommended improvements relating to CCTV and duress alarms. This was due to a lack of standardisation across DHHS, with a vast array of systems, software and providers engaged at the local level.

DHHS focused on implementing some physical rectifications, making little progress in addressing type four recommendations related to developing its organisational security culture through better processes and procedures.

Figure 2F shows DHHS's progress of security improvements as at July 2018.

Figure 2F
Progress of security improvements at DHHS as at July 2018

DHHS recommendation	Total number of recommendations	Per cent completed
Type one	8	75%
Type two	43	35%
Type three	135	37%
Type four	323	24%
All recommendations	509	27%

Note: Figures have been rounded.
Source: VAGO, based on documentation provided by DTF.

Without a proper security risk assessment of either agency to inform the improvements needed for security measures, it is not possible to ascertain whether the security measures implemented because of the RRAs and PSAs were the most appropriate or cost-effective.

3 Managing physical security

The government implements security measures to manage physical security risks and threats. All staff contribute to the effectiveness of these measures and play a role in security management. Security measures are most effective when staff promote a strong security culture.

Security measures should be commensurate with the level of risk. Common physical security measures implemented in Victorian Government office accommodation include:

- anti-jump barriers at lift wells
- CCTV and alarm monitoring
- a clear desk policy
- duress alarms
- identification passes
- mail and parcel delivery scanning
- security guards
- use of access cards
- visitor sign in and verification processes.

Antisocial behaviour, such as verbal abuse and threats to staff not causing physical harm, make up the majority of physical security incidents reported. A smaller number of even more serious incidents also occur.

Where a security measure is breached or ineffective, incident reporting and investigation is used to identify vulnerabilities and improve security measures to limit future incidents.

In this Part of the report, we assess how the SSP, DHHS and DJCS manage physical security measures and operations, including contract management, performance monitoring, how security is considered in accommodation planning, and how departments respond to security incidents.

3.1 Conclusion

Physical security management practices are still underdeveloped, both those for use at the state level and at the audited departments.

The security measures currently in place do not always effectively protect staff, government information and assets against such serious threats and risks. The government buildings we assessed have adequate physical security infrastructure to provide some defence against unauthorised access and antisocial behaviour. However, weaknesses in staff security culture and physical security procedures undermine the overall effectiveness of security measures against unauthorised access.

Currently, the state has limited visibility and control over the management of security services for government buildings. The SSP only manages security guarding services for a small number of government buildings, which means it does not have a complete picture of security risks and incidents in government buildings. Critically, the state relies on ad hoc guard reports to understand security incidents in government buildings. Incidents are not reported in buildings without guarding services, or where guards do not know about the incident. This means the state cannot quantify the magnitude of risks to its clients, its staff and the general public, across all buildings. The state also needs to better manage security guarding services through better performance measurement, incident reporting and investigation processes.

The statewide management of physical security also requires improvement. DTF needs to finalise the whole-of-government Accommodation Guidelines to include minimum security standards based on better practice, so that government staff and visitors can benefit from enhanced security in the future.

3.2 Physical security

We tested the adequacy of physical security measures at a selection of buildings occupied by government across regional and central Victoria.

While all tested sites have a range of physical security measures that control unauthorised access to some extent, security controls were bypassed and we accessed areas not permitted to the public. This enabled access to information and physical assets. We successfully accessed these sites because staff did not understand their role in maintaining physical security, or did not comply with established processes, allowing our testers access.

We also identified security risks that would result in significant breaches of physical security and we uncovered concerning information security practices. In one instance, we gained access to the master keys of a multi-tenanted building. In another, highly confidential information was found unsecured, outside of the immediate office area.

In addition to this, we observed several breaches and risks of a more moderate nature:

- Confidential information within the office space was not adequately secured or locked in lockers, tambours or filing cabinets.
- Staff did not always adhere to the clear desk policy, nor was it monitored or enforced by the department.
- There is not a strong practice of staff questioning or challenging unfamiliar or suspicious people in the office space.
- Staff were not aware or did not challenge those who tailgated them.
- The period of time that accessible gates remain open, and their use by able-bodied people for convenience.
- Workstations were often unlocked when unattended and passwords were left nearby on sticky notes.
- Lax processes for visitor or contractor sign in and approval.

Stronger governance processes and a positive security culture, in which all staff understand their role in maintaining physical security—as discussed in Part 2 of this report—would go a long way towards addressing these issues.

3.3 Accommodation planning

Effective physical security for office accommodation begins with a floorplan and facilities specifically designed to include physical security measures. It is easier and more effective to include measures from the design and planning stage, than to retrofit measures to a poorly designed office. Government departments with client-facing responsibilities also need to consider how physical security measures can safeguard its employees from occupational violence.

There is no assurance that the state is getting the best return on its investment in security through its accommodation planning. The existing guidelines on accommodation planning are outdated and the audited departments have taken different approaches to accommodation planning. Strategic leadership in this area is urgently required to ensure government agencies use better practice in their accommodation planning.

Department of Treasury and Finance

DTF sets out the minimum requirements for office accommodation, including some requirements for physical security, in its Accommodation Guidelines and Building Standards. These documents are used by government departments and agencies in the planning, leasing, fit-out and management of office accommodation. Departments may also create complementary or more detailed policies to suit their operational needs.

DTF has not reviewed the Accommodation Guidelines in more than 10 years. Since that time, the PSPF has been developed with guidelines for building security design. An update of DTF's Accommodation Guidelines commenced in 2009 but was never finalised. A second refresh began in July 2018. DTF has not confirmed when the new guidelines are expected to be completed and released. Once completed, DTF advises that the new guidelines will replace both the Accommodation Guidelines and the Building Standards.

The Accommodation Guidelines apply only to office accommodation and not to operational areas. Departments are responsible for the design of their operational areas, and any associated security measures. These areas include client interview and program rooms as well as areas accessible to the public, such as transaction counters and reception.

Department of Health and Human Services

DHHS does not have a formal process or set of consistent guidelines for office accommodation planning or design. Security planning is included in each site's design phase, based on the design brief. Design can be influenced by DHHS rather than directed by design standards.

The lack of strategy creates a potential that the designed security measures are not the most effective choice for the level of risk. It also does not provide assurance that security issues are adequately considered or that senior management has visibility of security considerations at an organisational level.

Department of Justice and Community Safety

DJCS uses DTF's guidelines as a base for its operational accommodation but has developed departmental accommodation planning guidelines and design standards for its offices. The guidelines apply to all accommodation built from late 2015 onwards. The guidelines also apply to any refurbishments to existing buildings.

The guidelines and standards balance the need for physical security with the need to create welcoming spaces for DJCS clients. The development of design specifications creates efficiency in the design process and ensures a consistent minimum approach to physical security.

Office accommodation leases

Victorian government offices are accommodated in a mixture of government-owned and privately leased premises.

Leasing with private landlords has economic benefits and allows government to remain within its preferred locations. However, it also creates risks for security management. While risk can never be eliminated, it needs to be mitigated as much as possible.

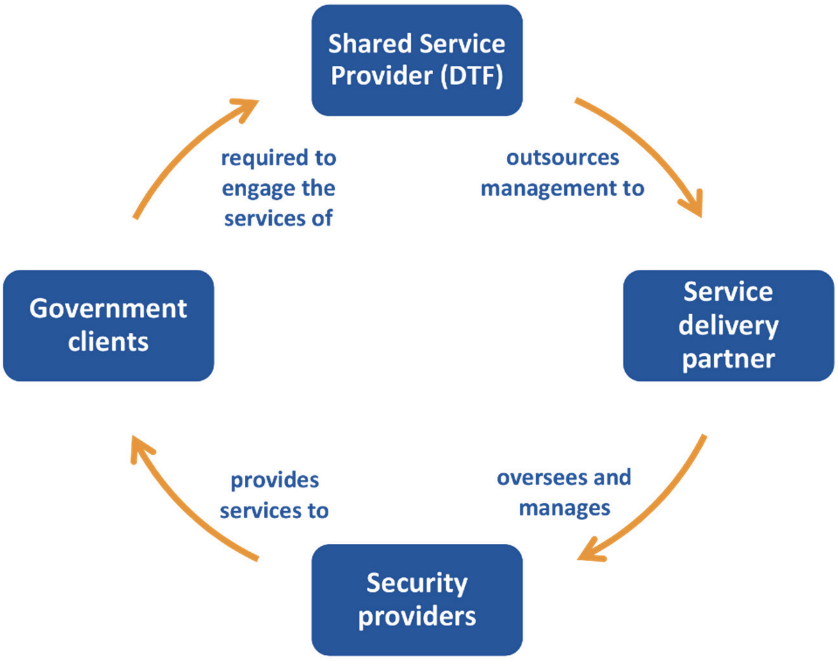
When leasing accommodation from private organisations, government may not always have input into the base building design and security measures. Government agencies can only control the security within their office space; for example, access control systems such as a swipe card system, or storage facilities. While certain physical security practices, such as turnstiles, may be better practice, they cannot be implemented without consent from the landlord. The SSP acknowledges that it has limited control over building access and the implementation of controls in private accommodation. Wherever possible, standards for baseline security measures should be built into lease agreements.

Further, private landlords often provide base building concierge and guarding services and have their own processes for occupational health and safety and security-related incidents. These processes mean that the SSP and the occupying government agencies do not have line of sight over incidents that occur within base building areas. One of the audited agencies noted an instance where the base building mail scanner was out of operation for three months without the building owner notifying the department or SSP. This lack of visibility over security issues weakens the SSP and department's efforts to monitor security risks and incidents.

3.4 Security services

There are four key types of stakeholders involved in the provision of security, as outlined in Figure 3A.

Figure 3A
Security services relationship cycle



Source: VAGO.

An effective security service should be flexible enough to respond to varying risk or threat levels and manage security incidents in a responsive and effective manner.

When the new SPC was established, the SSP provided departments with the option of adopting the suggested guarding arrangements for each site or revising aspects, such as the number or qualifications of the guards.

Most departments accepted the default arrangements, which means current security services may not be based on site-specific risk assessments.

Current security services are also limited in ensuring a safe and secure working environment because:

- they are based on a limited assessment of an organisation’s risks and vulnerabilities
- the security service’s operations have not been integrated into an organisation-wide risk management process, which is critically important to developing a security culture that promotes security being everyone’s business
- as highlighted in Section 3.3, the SSP has limited or no visibility of base building security operations.

Further, departments do not have access to provisions in the Security Services SPC and associated contracts, including provisions that directly impact on their ability to manage security. For example, departments do not have visibility of contractor performance or personnel security of guards at the department’s sites.

Management and oversight of security services

Effective performance monitoring is necessary to ensure that the security services offered are proportionate to the risks identified, and adequately mitigate security risks in day-to-day operations.

Oversight of the service delivery partner’s performance

The SSP’s service delivery partner is responsible for the management and oversight of 18 core services, including real estate, facilities, cleaning and waste, and security management. Despite security management services being one of those core services, its contract does not have specific key performance indicators (KPI) relating to this service. As a result, the SSP has no direct and specific mechanism to oversee the service delivery partner’s security management performance.

Although the SSP has novated management of security, to date it remains actively involved in operations and performance management. For example, the SSP is co-located with its service delivery partner, receives all incident reporting and attends the monthly operations meetings with the security providers. While these are operationally sound practices, there are limited formal mechanisms to review the service delivery partner’s performance in security.

Performance monitoring of security providers

The SSP’s performance monitoring of security services heavily relies on client complaints and exception-based reporting, making it difficult to evaluate whether its responses are timely. The current security services’ KPIs and management reports need to be improved.

The security providers are subject to five KPIs, as shown in Figure 3B.

Figure 3B
Security services' KPIs

Service element	Description	KPI/source of data
Use of registered officers	Service delivery personnel have the necessary qualifications, checks and up-to-date training.	Monthly roster of personnel per site compared to register log
Security officers fit for duty	All personnel are suitably qualified and trained to meet the contract's technical specification. One hundred per cent of service delivery personnel have documented transition training.	Audits, personnel training records
Provision of agreed services	Services provided are in accordance with the site requirements as set out in the contract's specification and through the agreed standard operating procedures.	Contractor's complaint log
Incident response	All issues and complaints are responded to in a timely manner: • 100 per cent of instances are to be acknowledged and reported within 24 hours • 100 per cent of instances are to be resolved within 20 working days of acknowledgement, or as agreed with the SSP.	Contractor's incident and complaint log
Complaints handling	Complaints actioned and resolved in accordance with site requirements and within the agreed period as set out in the technical specification. The default period is one day.	Contractor's incident and complaint log

Source: VAGO, based on the Security Services SPC.

The current KPIs do not provide sufficient and relevant information for security operations. There are several deficiencies in the KPI measures:

- Performance in the element 'provision of agreed services' is measured by the number of complaints received. Compliance in any given month is defined as no more than three valid compliance issues. The 'agreed services' may include a range of security services, such as guarding, mail room and control room operations, and each requires a different performance measurement. The current indicator is not a specific measure of the agreed range of operations and it cannot indicate which service might have issues.
- Complaints are not risk-rated, making it difficult—based on KPI information only—to gauge if non-compliance in a service area is critical or not.
- Incidents do not have a risk rating and incident responses do not have risk-based time frames. In security operations, a risk-based approach is critically important to reporting and responding to incidents. The SSP observed some instances where incidents were not reported in a timely way.

The SSP has standardised the monthly operations report template for security providers, which is an improvement on the previous contract.

We reviewed six of the monthly operations reports and corresponding meeting minutes between the SSP, the service delivery partner and security providers. We noted that the monthly reports require further improvements in the consistency and quality of the information presented. For example:

- Some risk classifications are illogical and inconsistent; for example, sites frequented by ministers were erroneously marked as low risk.
- Some KPIs that measure compliance with a score of either 'met' or 'fail' are reported in percentages.
- Certain fields in the report are not accurately completed by the security provider and sometimes not at all.
- Some reports were not signed by the security contractor or SSP representative to acknowledge that the information provided was accurate.

The SSP acknowledges the deficiencies in the monthly performance meetings and KPI reports, and states they are still refining them. While the reports could be a useful tool for performance monitoring discussions, the lack of quality control casts doubt as to whether the reports are used meaningfully.

Although a contractual requirement, both the service delivery partner and security service providers do not undertake regular site audits. The SSP advise that on occasion they have observed issues and raised them with the service providers. For example, guards not stationed at turnstiles as per the standing orders. The SSP should ensure that the service delivery partner and security service providers carry out site audits to complement the KPI and monthly reports.

Statewide visibility and control

Currently the state has limited visibility and control over how security services for government buildings are managed.

The Security Services SPC was established to deliver benefits to the state, including to:

- maximise cost efficiencies
- increase the quality of security services and level of protection to reduce the risk of security incidents occurring
- improve the visibility and control of government security procurement requirements for labour, equipment and maintenance.

The SSP's reach over the management of government building security services is limited:

- The SSP is aware that some government agencies, independent of the SSP, have arranged security services under the SPC for their office accommodation. The SSP does not know how many government agencies do this because there is no requirement for agencies to report a contract that is valued under $100 000. As a result, the SSP does not have a statewide overview of security services for all government buildings.
- There is no SPC panel for security equipment, such as alarms and cameras, and their maintenance. Each department currently procures these items independently or on an ad hoc basis. However, cost savings are likely when aggregating these services. For example, the SSP advised that one government agency brought its alarm monitoring services across its various sites under one contract and has been able to achieve cost-efficiency, while improving security control and visibility.

3.5 Security incidents

Security incidents are events that could have or did compromise the safety of people or the availability, confidentiality or value of government information or assets. An incident with malicious intent can occur when someone gains unauthorised access to a government building, to cause harm to staff or seize sensitive information. This can result from an intruder targeting weak physical security infrastructure—such entering unnoticed through a door that is unsecured or kept open—or by taking advantage of negligent behaviour—such as gaining access because procedures to sign-in visitors to a government building are ignored. Accurate recording and effective monitoring and evaluation of security incidents can assist departments in identifying trends and weaknesses in security measures and provide insight into performance and incident management.

Incident reporting and monitoring

The Victorian Government does not currently have an accurate understanding of the nature or volume of physical, or protective security incidents.

DHHS, DJCS, and the SSP do not have mature incident reporting and monitoring procedures or systems. They have implemented incident reporting and monitoring to varying degrees.

Shared Service Provider

The SSP's incident reporting and monitoring process has improved under the recent SPC but requires further development and improvement.

Under the current Security Services SPC, security providers are required to report incidents to the SSP by the end of the officer's shift. Incidents are only reported when observed, reported or attended to, by a guard. However, not all locations have guarding services. There are no mechanisms for employees or visitors to report incidents to the SSP. Because of this, the incidents reported are not a complete record and cannot be relied on for comparative analysis, either between sites or departments.

Guards submit incident reports using an SSP-supplied template. The template standardises incident reporting across service suppliers and includes a consistent category of incidents. The incident reporting template would benefit from a corresponding incident classification guide. It is difficult to differentiate between many of the incident types based solely on the incident name; for example, 'security access', 'access control' and 'unauthorised access' or 'irate/abusive behaviour' and 'violent behaviour'.

While all incidents are security related, some are occurrences—events for noting, rather than incidents—or occupational health and safety matters. Incidents are not rated for risk or impact, meaning there is no easy way to differentiate between incidents that are 'occurrences' or incidents of greater significance.

This incident reporting process is an improvement on the former Security Services SPC, in which the SSP accepted incident reporting in different formats and to differing standards of quality.

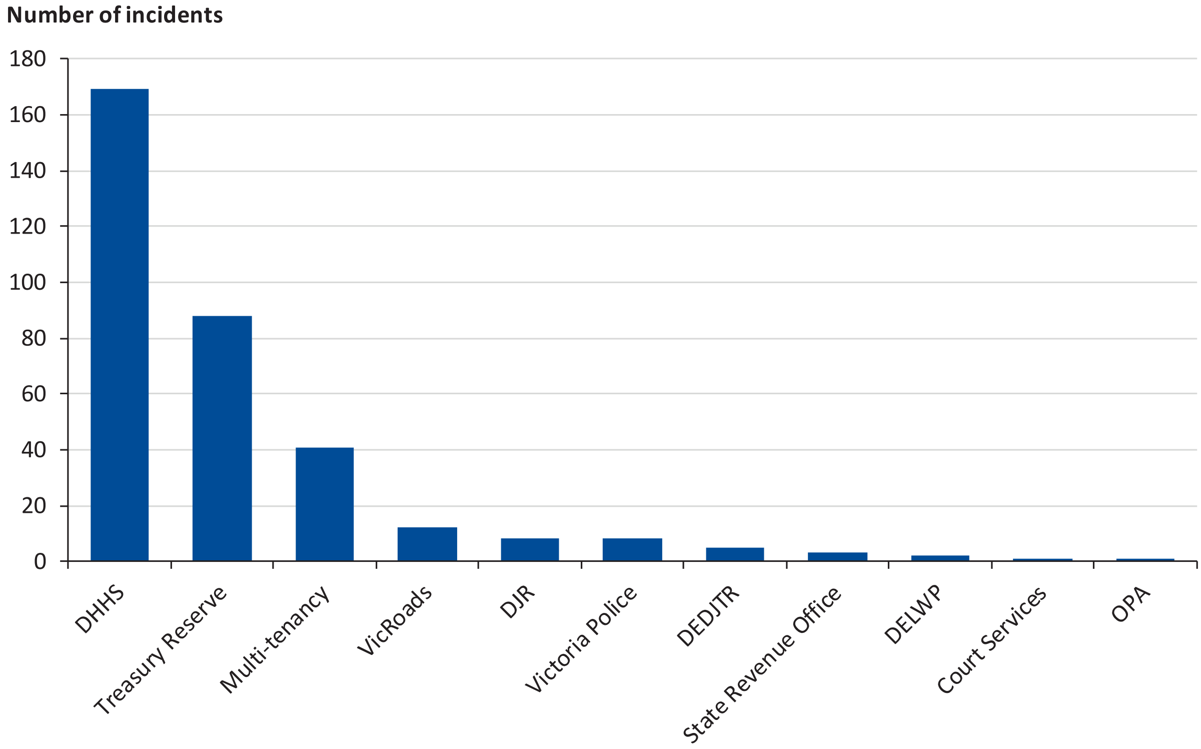
Incident dashboard

The SSP began collating incident reports into a dashboard format in July 2017. There are dashboards for each of the agencies managed by the SSP as well as a statewide dashboard. It includes metrics such as:

- number of incidents by incident category and month
- percentage of incident types
- incident types by location
- number of emergency services calls
- number of incident reports by service provider (statewide dashboard only).

Figure 3C shows the number of security incidents reported to the SSP by each agency but should be interpreted with caution for the reasons previously outlined.

Figure 3C
Security incidents reported to the SSP by agency, January to December 2018

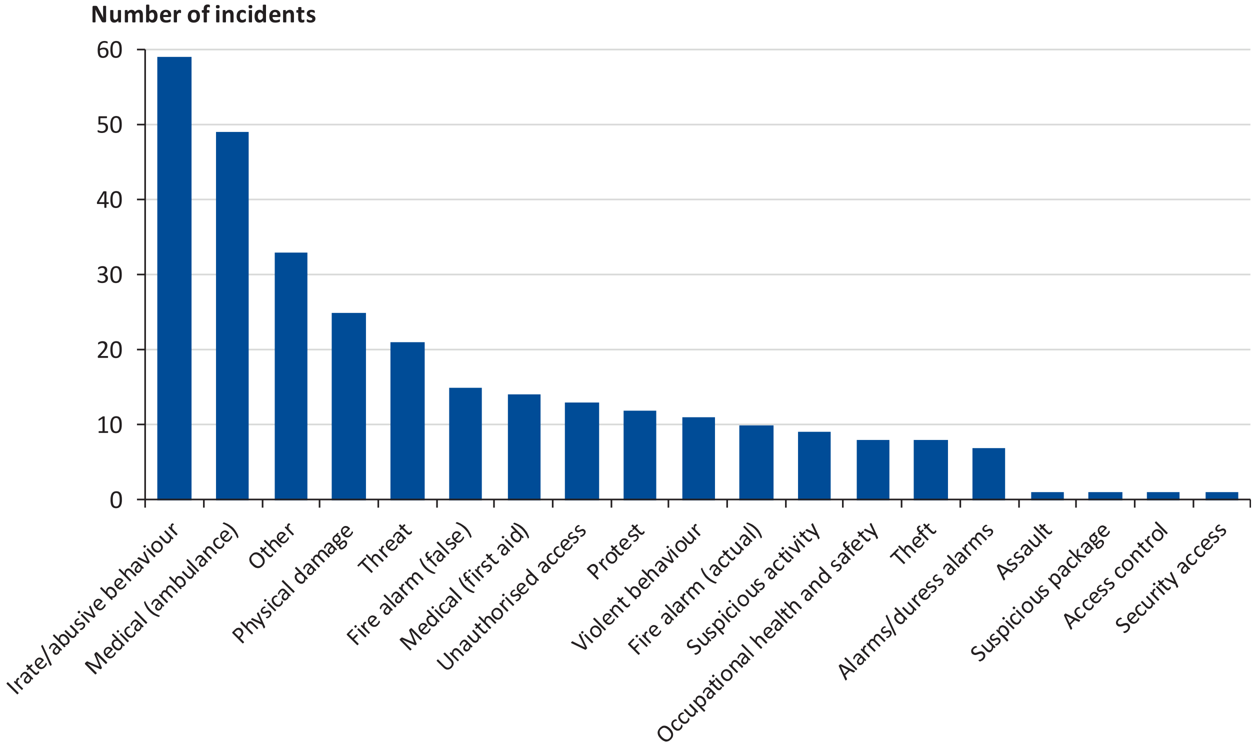


Note: Treasury Reserve is a precinct of government buildings within Treasury Place, Spring Street, Macarthur Street, St Andrews Place and Lansdowne Street; DJR is the former Department of Justice and Regulation; DEDJTR is the former Department of Economic Development, Jobs, Transport and Resources; DELWP is the Department of Environment, Land, Water and Planning; OPA is the Office of the Public Advocate.
Source: VAGO, based on incident data provided by DTF.

According to Figure 3C, a disproportionate number of incidents were reported at DHHS locations. In 2018, 169 DHHS incidents were reported. This is likely because DHHS has guards at most of its service centres, unlike DJCS. It is almost certain that incidents are occurring within the office accommodation of the other government agencies in Figure 3C; however, these would not be captured by the SSP as these agencies have fewer or no guards.

Figure 3D is a breakdown of the number of incidents by incident classification.

Figure 3D
Incidents reported to the SSP by classification, July to December 2018



Source: VAGO, based on incident data provided by DTF.

Figure 3D shows that the most common incident type relates to staff safety. Between July and December 2018 there were 59 reports of irate and abusive behaviour. Medical incidents were also common, with 49 reported ambulance call-outs in the same period. While medical incidents are a type of safety incident, they are not necessarily related to security. Incidents relating to the physical security of office accommodation such as unauthorised access, access control, suspicious activity or suspicious packages were reported less frequently but have still occurred in this six-month period.

The SSP has only 18 months of incident data available, which is not enough to undertake reliable trend analysis. However, comparison between regional/rural and CBD office accommodation over the 18 months shows that the most prominent type of incident varies by location. In the CBD, which is mostly corporate office accommodation, medical incidents and the activation of fire alarms were the most common. In regional locations, which offer services to clients, incidents relating to irate or abusive behaviour were the most common.

The SSP does not currently have a formal process to share the incident dashboard with departments, but stated it intends to share snapshots of it with departments twice a year.

Departments

Departments should not rely solely on the SSP's incident reporting, but instead use it to supplement and compare with their own incident reports. As required by the SPC, the SSP only receives incidents if they were observed by, reported to, or attended by a guard. Realistically, only a small number of incidents would be reported to the SSP as most government offices do not have guards. Government staff and contractors also observe many potential security incidents but there are no processes to report these to the SSP. For accurate incident reporting, departments must ensure all personnel understand how to report real or perceived incidents, and why it is important to do so. This not only requires incident reporting procedures, but also staff training and education.

DHHS does not have a process to collect and record physical security incidents but has reporting systems for other types of incidents, such as occupational health and safety and client incidents. These separate systems are not integrated and DHHS does not aggregate or analyse the data generated.

DJCS has developed a process for systematic incident reporting, monitoring, review and evaluation through the Security Incident Response Centre (SIRC). This process is new and not yet embedded and consistently used across DJCS and its regions. Its standard operating procedure for security incident management outlines how the SIRC will function once fully implemented.

Incidents reported to the SIRC are compiled into a register that records incident details, management, outcomes and any investigation or evaluation. In future, this will be used for trend analysis and reporting to its security governance committees.

Investigation and evaluation

A security investigation is the formal process of evaluating the causes and consequences of an actual or perceived security incident that has, or could have, caused harm to an individual, the organisation, its assets or information. Not every security incident will require a formal investigation. It is at the discretion of each agency to decide whether an incident is significant enough for investigation.

The investigation of incidents is an important step in addressing vulnerabilities and improving staff culture for the future. The investigation can gather evidence for corrective, criminal or civil action. A security investigation may result in improved security measures, procedures, or response management or may affirm the action already taken.

None of the three agencies involved in this audit routinely investigate and evaluate security incidents. DJCS first developed incident investigation and evaluation procedures in July 2018 and was the only audited agency that has done so, however they are still in draft form. This is a lost opportunity to learn from previous incidents and improve or modify security measures.

Shared Service Provider

The SSP currently reviews all reported incidents but does not routinely investigate or evaluate security incidents. The SSP has advised that, where necessary, onsite security may follow up incidents to ascertain further detail. If further investigation is required, this is the responsibility of both the SSP and the department or agency at which the incident occurred.

Department of Justice and Community Safety

Like its incident reporting processes, DJCS is currently finalising and implementing its security incident review and evaluation procedures. The process, which is documented in a draft Security Incident Investigation Manual and Security Incident Management Standard Operating Procedure, outlines a risk-based approach. DJCS already has established processes for other types of investigations.

Not all incidents require investigation. At present, the decision to investigate is not guided by any formal criteria but is a judgement made by DJCS's Agency Security Advisor. DJCS intends to develop formal criteria in future. There are draft risk assessment forms that provide guidance on:

- the level of management/executive the incident is reported to
- the level of management/executive the incident is monitored by
- whether implementing remedial treatments is necessary or discretionary.

The manual also requires that progress on implementing recommendations be reported on within a specified time frame.

In addition to this, DJCS follows up on incidents reported to them by the SSP.

Department of Health and Human Services

DHHS does not have a documented process for investigating or evaluating physical security incidents. Only a small number of critical incidents are investigated on an ad hoc basis at the request of senior management.

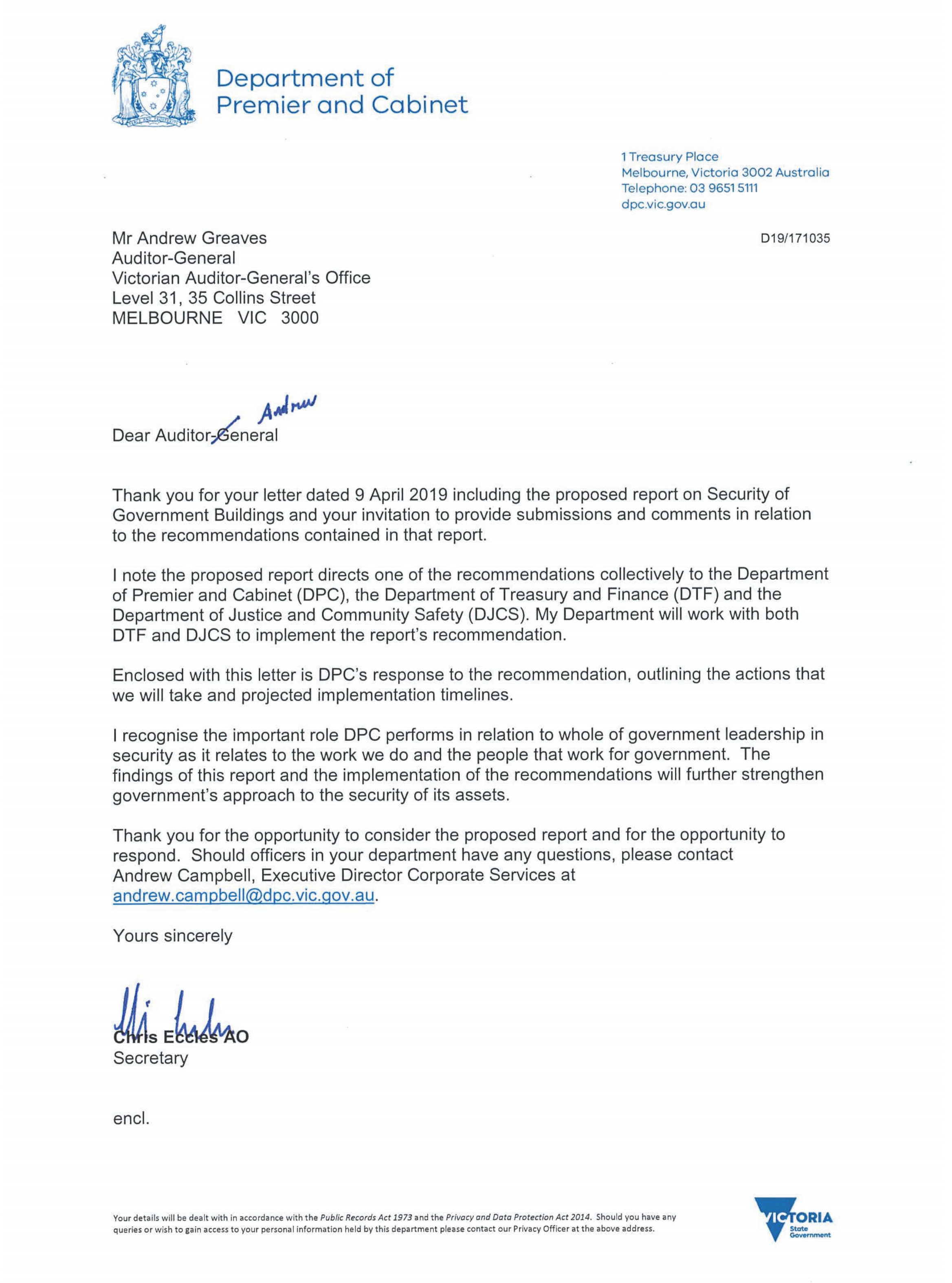
Appendix A *Audit Act 1994* section 16—submissions and comments

We have consulted with DTF, DHHS, DJCS, and DPC and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report to those agencies and asked for their submissions and comments.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

RESPONSE provided by the Secretary, DPC



Department of
Premier and Cabinet

1 Treasury Place
Melbourne, Victoria 3002 Australia
Telephone: 03 9651 5111
dpc.vic.gov.au

D19/171035

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

Dear ~~Auditor-General~~ Andrew

Thank you for your letter dated 9 April 2019 including the proposed report on Security of Government Buildings and your invitation to provide submissions and comments in relation to the recommendations contained in that report.

I note the proposed report directs one of the recommendations collectively to the Department of Premier and Cabinet (DPC), the Department of Treasury and Finance (DTF) and the Department of Justice and Community Safety (DJCS). My Department will work with both DTF and DJCS to implement the report's recommendation.

Enclosed with this letter is DPC's response to the recommendation, outlining the actions that we will take and projected implementation timelines.

I recognise the important role DPC performs in relation to whole of government leadership in security as it relates to the work we do and the people that work for government. The findings of this report and the implementation of the recommendations will further strengthen government's approach to the security of its assets.

Thank you for the opportunity to consider the proposed report and for the opportunity to respond. Should officers in your department have any questions, please contact Andrew Campbell, Executive Director Corporate Services at andrew.campbell@dpc.vic.gov.au.

Yours sincerely

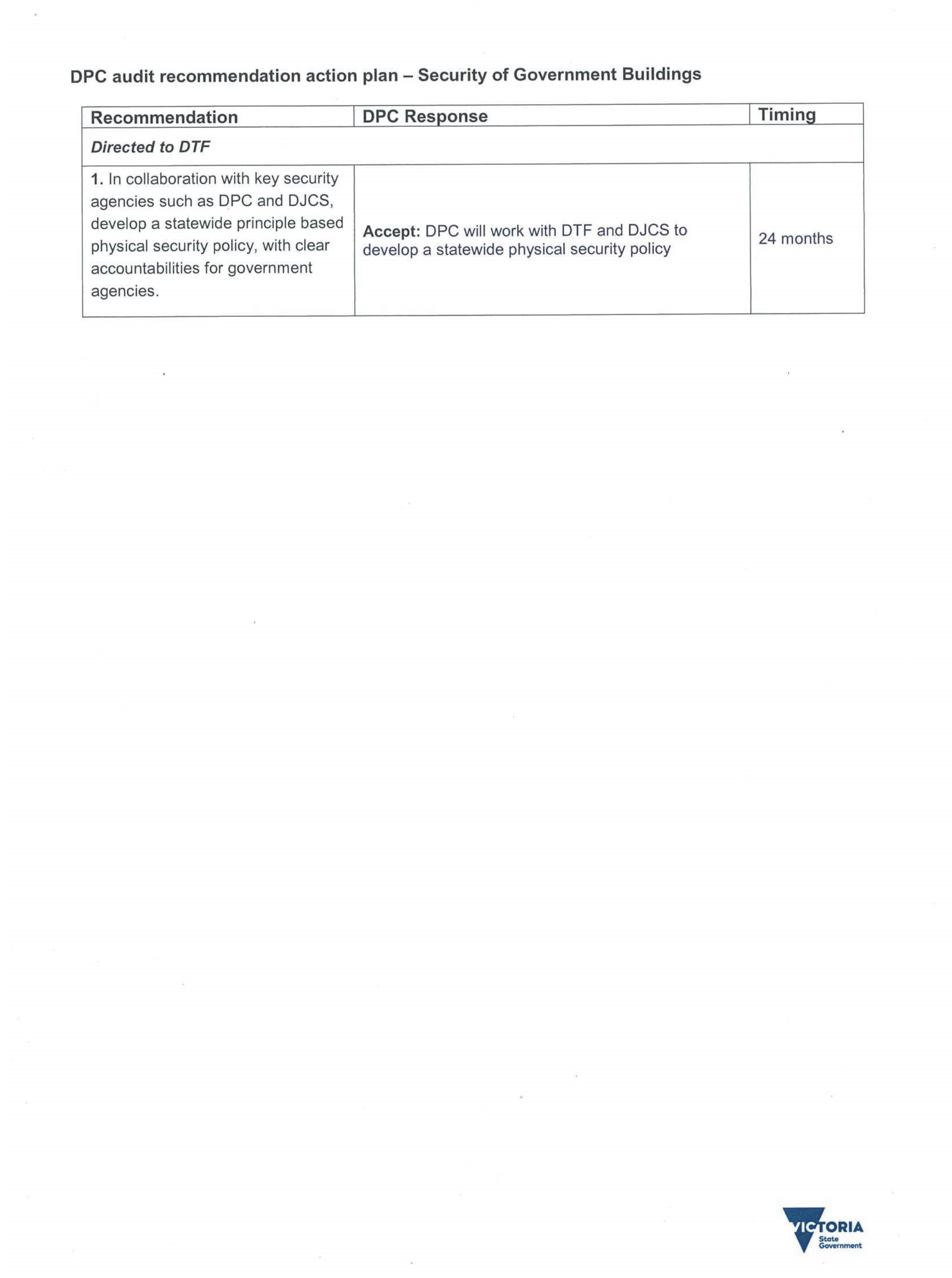
Chris Eccles AO
Secretary

encl.

Your details will be dealt with in accordance with the *Public Records Act 1973* and the *Privacy and Data Protection Act 2014*. Should you have any queries or wish to gain access to your personal information held by this department please contact our Privacy Officer at the above address.

VICTORIA State Government

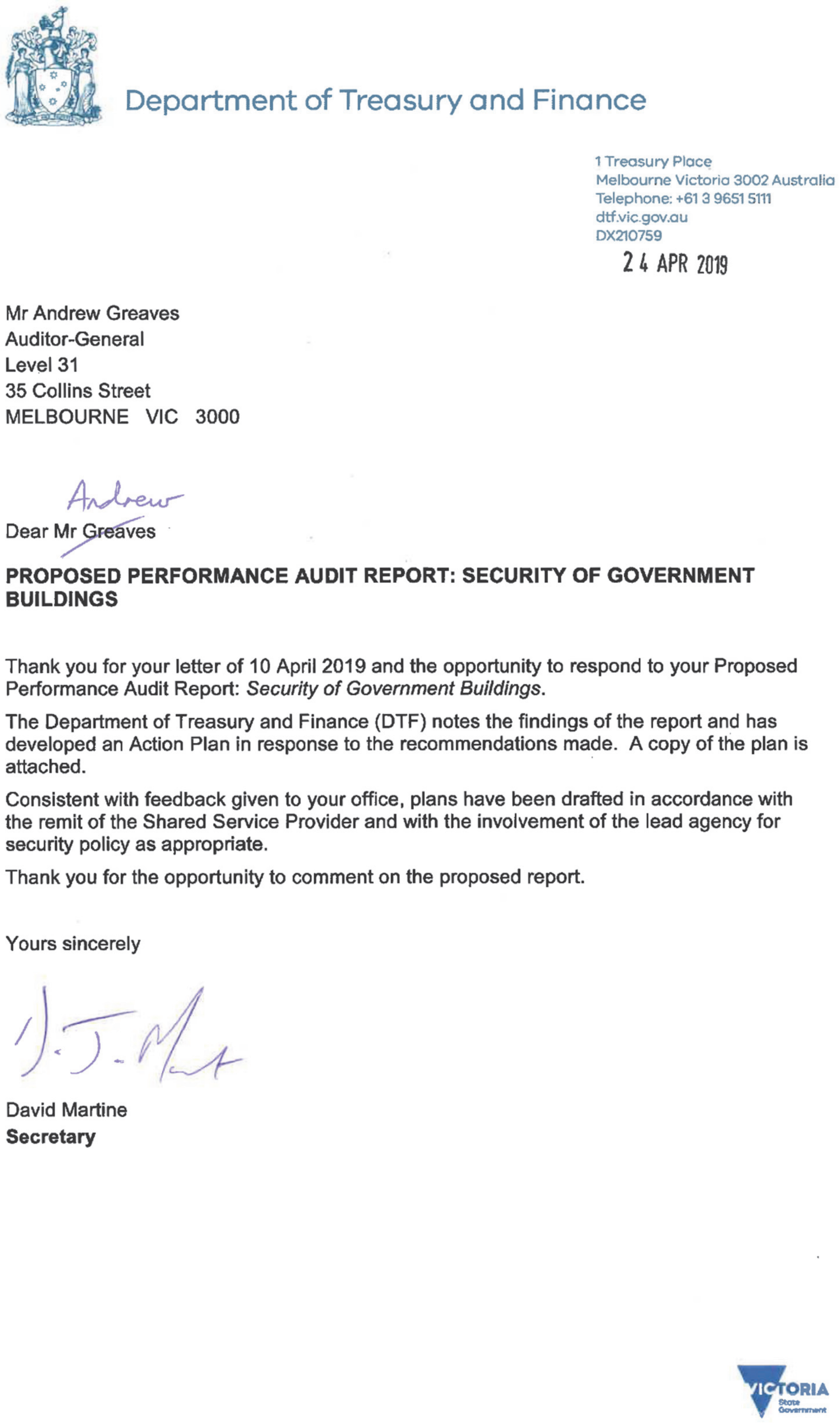
RESPONSE provided by the Secretary, DPC—continued



DPC audit recommendation action plan – Security of Government Buildings

Recommendation	DPC Response	Timing
Directed to DTF		
1. In collaboration with key security agencies such as DPC and DJCS, develop a statewide principle based physical security policy, with clear accountabilities for government agencies.	**Accept:** DPC will work with DTF and DJCS to develop a statewide physical security policy	24 months

RESPONSE provided by the Secretary, DTF



Department of Treasury and Finance

1 Treasury Place
Melbourne Victoria 3002 Australia
Telephone: +61 3 9651 5111
dtf.vic.gov.au
DX210759

24 APR 2019

Mr Andrew Greaves
Auditor-General
Level 31
35 Collins Street
MELBOURNE VIC 3000

Dear Mr ~~Greaves~~ Andrew

PROPOSED PERFORMANCE AUDIT REPORT: SECURITY OF GOVERNMENT BUILDINGS

Thank you for your letter of 10 April 2019 and the opportunity to respond to your Proposed Performance Audit Report: *Security of Government Buildings*.

The Department of Treasury and Finance (DTF) notes the findings of the report and has developed an Action Plan in response to the recommendations made. A copy of the plan is attached.

Consistent with feedback given to your office, plans have been drafted in accordance with the remit of the Shared Service Provider and with the involvement of the lead agency for security policy as appropriate.

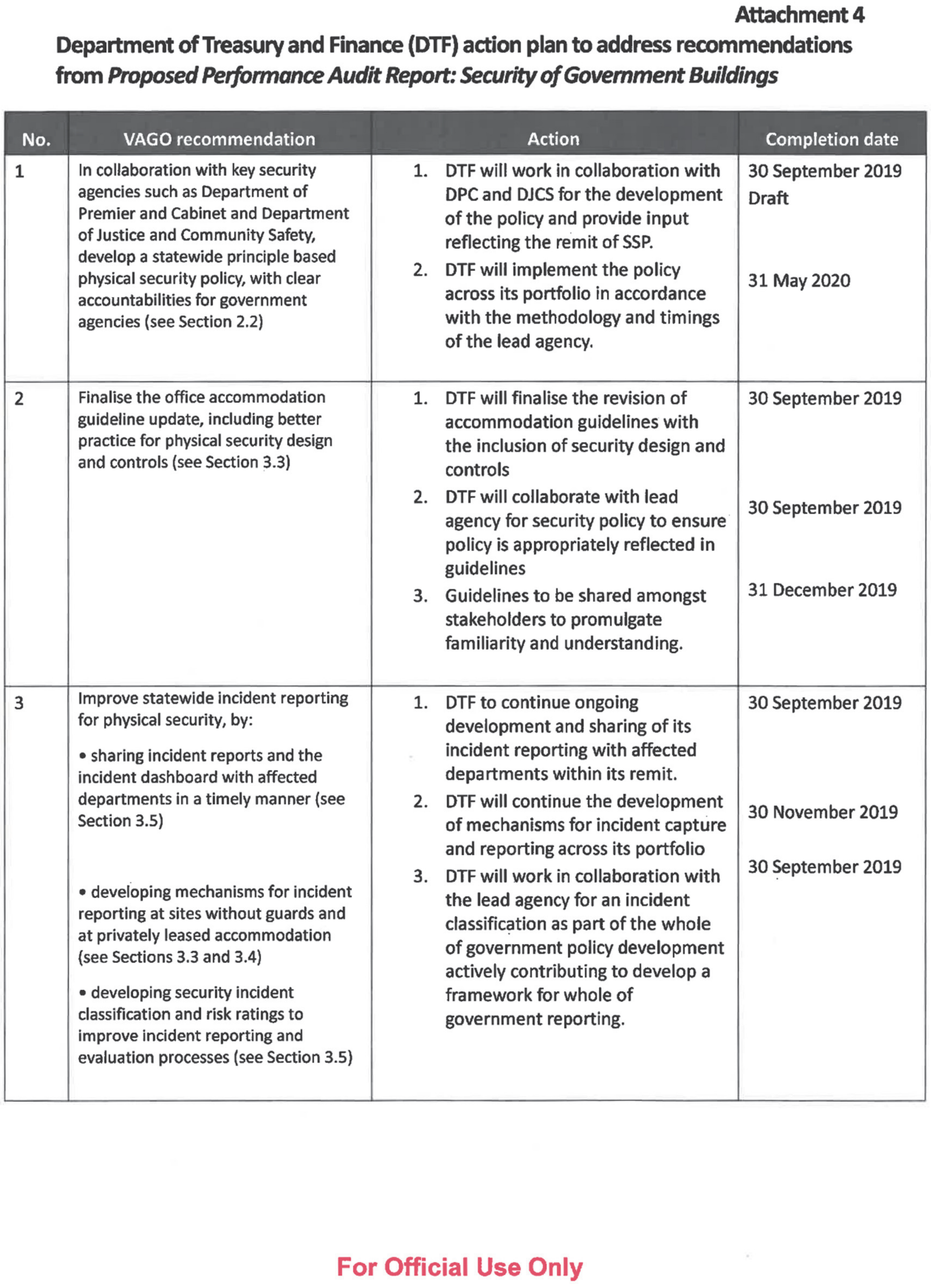
Thank you for the opportunity to comment on the proposed report.

Yours sincerely

David Martine
Secretary

VICTORIA State Government

RESPONSE provided by the Secretary, DTF—continued



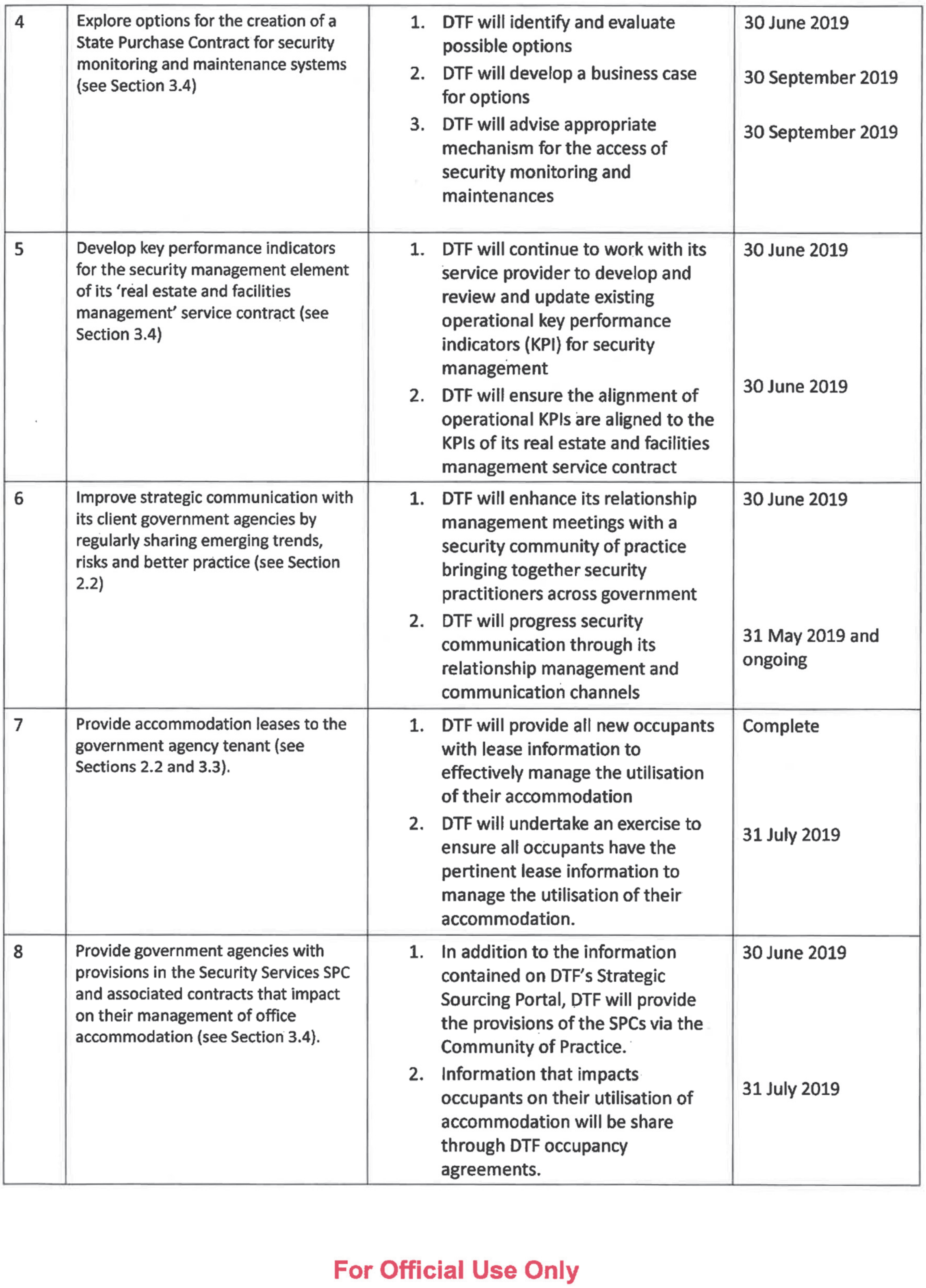
Attachment 4

Department of Treasury and Finance (DTF) action plan to address recommendations from *Proposed Performance Audit Report: Security of Government Buildings*

No.	VAGO recommendation	Action	Completion date
1	In collaboration with key security agencies such as Department of Premier and Cabinet and Department of Justice and Community Safety, develop a statewide principle based physical security policy, with clear accountabilities for government agencies (see Section 2.2)	1. DTF will work in collaboration with DPC and DJCS for the development of the policy and provide input reflecting the remit of SSP. 2. DTF will implement the policy across its portfolio in accordance with the methodology and timings of the lead agency.	30 September 2019 Draft 31 May 2020
2	Finalise the office accommodation guideline update, including better practice for physical security design and controls (see Section 3.3)	1. DTF will finalise the revision of accommodation guidelines with the inclusion of security design and controls 2. DTF will collaborate with lead agency for security policy to ensure policy is appropriately reflected in guidelines 3. Guidelines to be shared amongst stakeholders to promulgate familiarity and understanding.	30 September 2019 30 September 2019 31 December 2019
3	Improve statewide incident reporting for physical security, by: • sharing incident reports and the incident dashboard with affected departments in a timely manner (see Section 3.5) • developing mechanisms for incident reporting at sites without guards and at privately leased accommodation (see Sections 3.3 and 3.4) • developing security incident classification and risk ratings to improve incident reporting and evaluation processes (see Section 3.5)	1. DTF to continue ongoing development and sharing of its incident reporting with affected departments within its remit. 2. DTF will continue the development of mechanisms for incident capture and reporting across its portfolio 3. DTF will work in collaboration with the lead agency for an incident classification as part of the whole of government policy development actively contributing to develop a framework for whole of government reporting.	30 September 2019 30 November 2019 30 September 2019

For Official Use Only

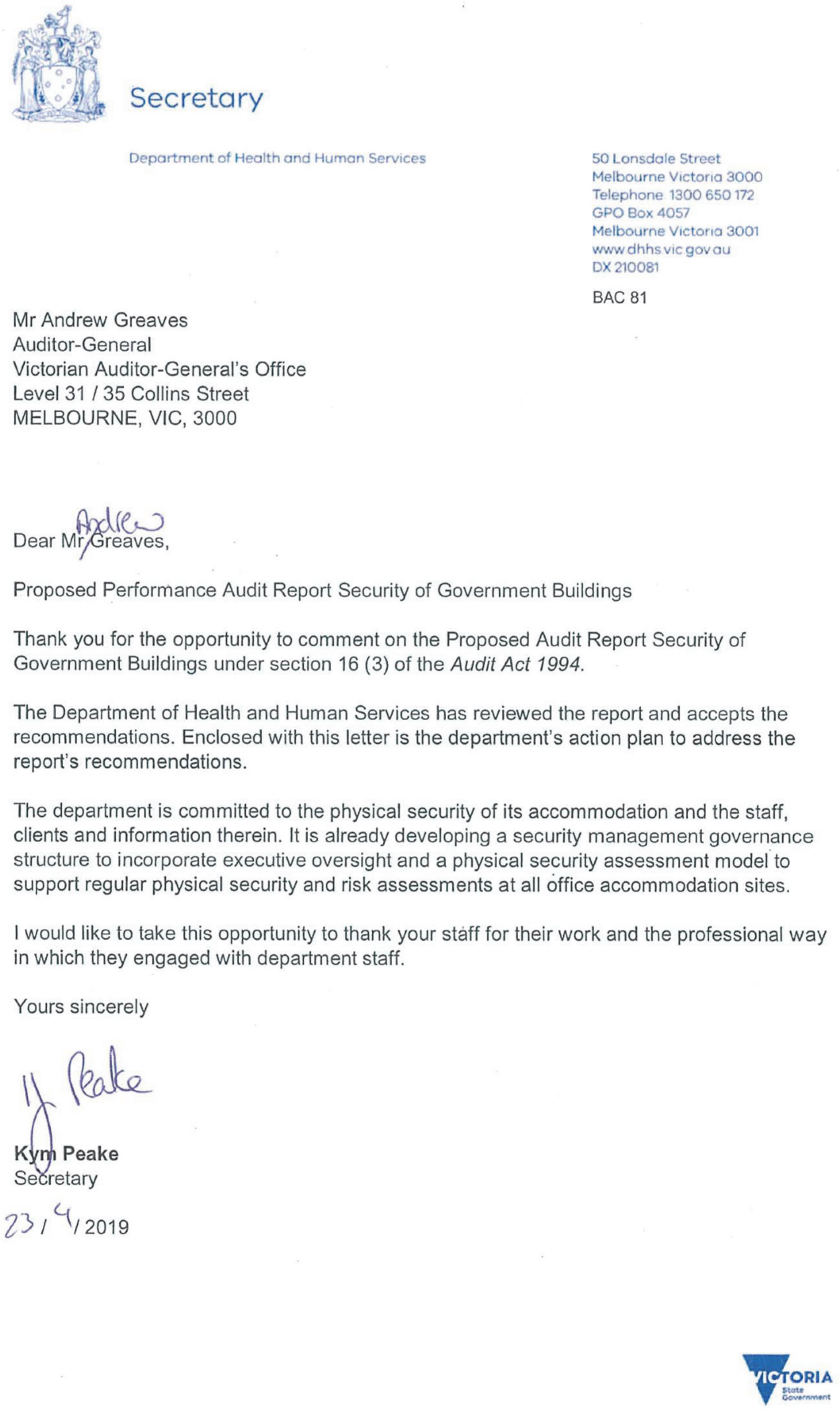
RESPONSE provided by the Secretary, DTF—continued



4	Explore options for the creation of a State Purchase Contract for security monitoring and maintenance systems (see Section 3.4)	1. DTF will identify and evaluate possible options 2. DTF will develop a business case for options 3. DTF will advise appropriate mechanism for the access of security monitoring and maintenances	30 June 2019 30 September 2019 30 September 2019
5	Develop key performance indicators for the security management element of its 'real estate and facilities management' service contract (see Section 3.4)	1. DTF will continue to work with its service provider to develop and review and update existing operational key performance indicators (KPI) for security management 2. DTF will ensure the alignment of operational KPIs are aligned to the KPIs of its real estate and facilities management service contract	30 June 2019 30 June 2019
6	Improve strategic communication with its client government agencies by regularly sharing emerging trends, risks and better practice (see Section 2.2)	1. DTF will enhance its relationship management meetings with a security community of practice bringing together security practitioners across government 2. DTF will progress security communication through its relationship management and communication channels	30 June 2019 31 May 2019 and ongoing
7	Provide accommodation leases to the government agency tenant (see Sections 2.2 and 3.3).	1. DTF will provide all new occupants with lease information to effectively manage the utilisation of their accommodation 2. DTF will undertake an exercise to ensure all occupants have the pertinent lease information to manage the utilisation of their accommodation.	Complete 31 July 2019
8	Provide government agencies with provisions in the Security Services SPC and associated contracts that impact on their management of office accommodation (see Section 3.4).	1. In addition to the information contained on DTF's Strategic Sourcing Portal, DTF will provide the provisions of the SPCs via the Community of Practice. 2. Information that impacts occupants on their utilisation of accommodation will be share through DTF occupancy agreements.	30 June 2019 31 July 2019

For Official Use Only

RESPONSE provided by the Secretary, DHHS



Secretary

Department of Health and Human Services

50 Lonsdale Street
Melbourne Victoria 3000
Telephone 1300 650 172
GPO Box 4057
Melbourne Victoria 3001
www.dhhs.vic.gov.au
DX 210081

BAC 81

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31 / 35 Collins Street
MELBOURNE, VIC, 3000

Dear ~~Mr Greaves~~ Andrew,

Proposed Performance Audit Report Security of Government Buildings

Thank you for the opportunity to comment on the Proposed Audit Report Security of Government Buildings under section 16 (3) of the *Audit Act 1994*.

The Department of Health and Human Services has reviewed the report and accepts the recommendations. Enclosed with this letter is the department's action plan to address the report's recommendations.

The department is committed to the physical security of its accommodation and the staff, clients and information therein. It is already developing a security management governance structure to incorporate executive oversight and a physical security assessment model to support regular physical security and risk assessments at all office accommodation sites.

I would like to take this opportunity to thank your staff for their work and the professional way in which they engaged with department staff.

Yours sincerely

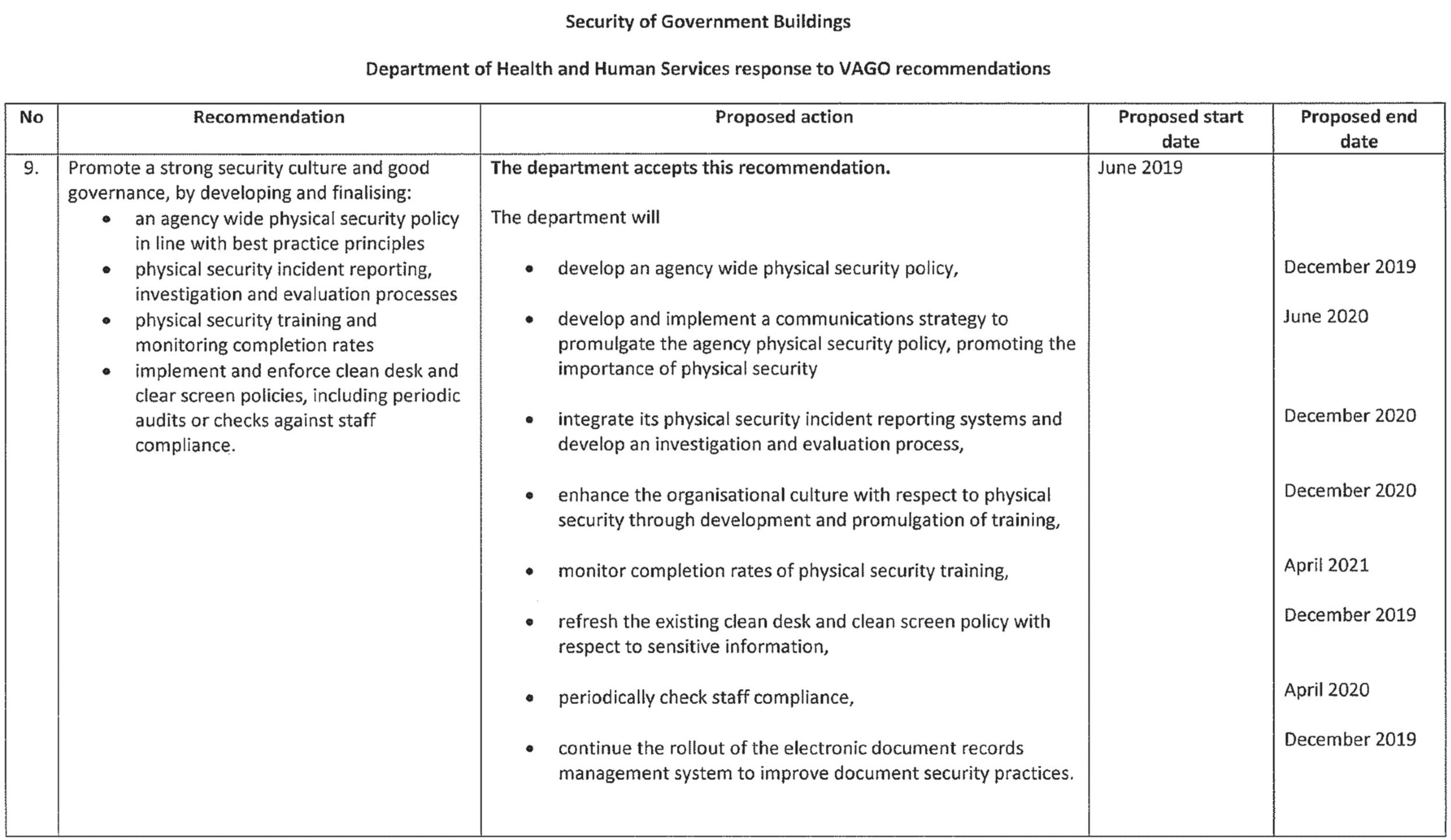
K Peake

Kym Peake
Secretary

23 / 4 / 2019

VICTORIA
State Government

RESPONSE provided by the Secretary, DHHS—continued



Security of Government Buildings

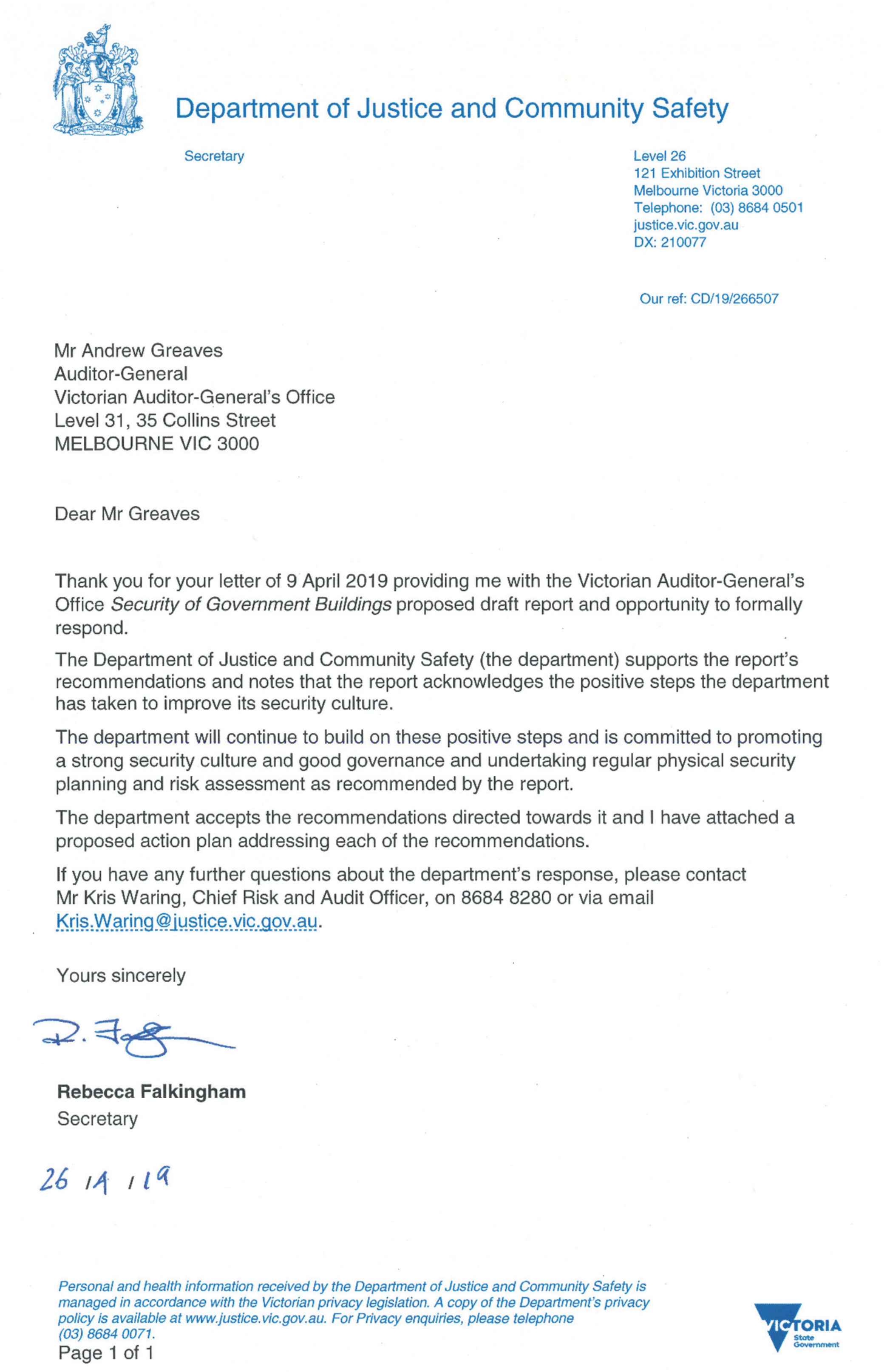
Department of Health and Human Services response to VAGO recommendations

No	Recommendation	Proposed action	Proposed start date	Proposed end date
9.	Promote a strong security culture and good governance, by developing and finalising: • an agency wide physical security policy in line with best practice principles • physical security incident reporting, investigation and evaluation processes • physical security training and monitoring completion rates • implement and enforce clean desk and clear screen policies, including periodic audits or checks against staff compliance.	**The department accepts this recommendation.** The department will	June 2019	
		• develop an agency wide physical security policy,		December 2019
		• develop and implement a communications strategy to promulgate the agency physical security policy, promoting the importance of physical security		June 2020
		• integrate its physical security incident reporting systems and develop an investigation and evaluation process,		December 2020
		• enhance the organisational culture with respect to physical security through development and promulgation of training,		December 2020
		• monitor completion rates of physical security training,		April 2021
		• refresh the existing clean desk and clean screen policy with respect to sensitive information,		December 2019
		• periodically check staff compliance,		April 2020
		• continue the rollout of the electronic document records management system to improve document security practices.		December 2019

RESPONSE provided by the Secretary, DHHS—continued

10.	Undertake regular physical security planning and risk assessment.	**The department accepts this recommendation.** The department is developing a physical security assessment model and will undertake regular physical security and risk assessments at all office accommodation sites. The first audit will incorporate all client servicing office accommodation sites and identified key sites. Concurrently with the first audit, the department will develop an over-arching risk management profile for the department's office accommodation portfolio. Subsequent audits will be conducted regularly in line with the agreed risk management profile.	Commenced	December 2019
11.	Develop design standards for accommodation planning and office refurbishments at client facing locations, incorporating minimum security measures and controls.	**The department accepts this recommendation.** The department will develop design standards for client servicing office accommodation that incorporates, in order of priority public reception and waiting areas (Zone 1); client interface rooms/areas (Zone 2); and secure staff areas (Zone 3) These standards will be designed with the operations divisions and will incorporate the appropriate minimum-security measures and controls in line with the individual site's overall risk profile.	June 2019	December 2020
12.	Develop a governance structure for security management, including clear accountability and adequate executive oversight.	**The department accepts this recommendation.** The department is developing a security management governance structure to provide clear accountability and executive oversight.	Commenced	September 2019

RESPONSE provided by the Secretary, DJCS



Department of Justice and Community Safety

Secretary

Level 26
121 Exhibition Street
Melbourne Victoria 3000
Telephone: (03) 8684 0501
justice.vic.gov.au
DX: 210077

Our ref: CD/19/266507

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

Dear Mr Greaves

Thank you for your letter of 9 April 2019 providing me with the Victorian Auditor-General's Office *Security of Government Buildings* proposed draft report and opportunity to formally respond.

The Department of Justice and Community Safety (the department) supports the report's recommendations and notes that the report acknowledges the positive steps the department has taken to improve its security culture.

The department will continue to build on these positive steps and is committed to promoting a strong security culture and good governance and undertaking regular physical security planning and risk assessment as recommended by the report.

The department accepts the recommendations directed towards it and I have attached a proposed action plan addressing each of the recommendations.

If you have any further questions about the department's response, please contact Mr Kris Waring, Chief Risk and Audit Officer, on 8684 8280 or via email Kris.Waring@justice.vic.gov.au.

Yours sincerely

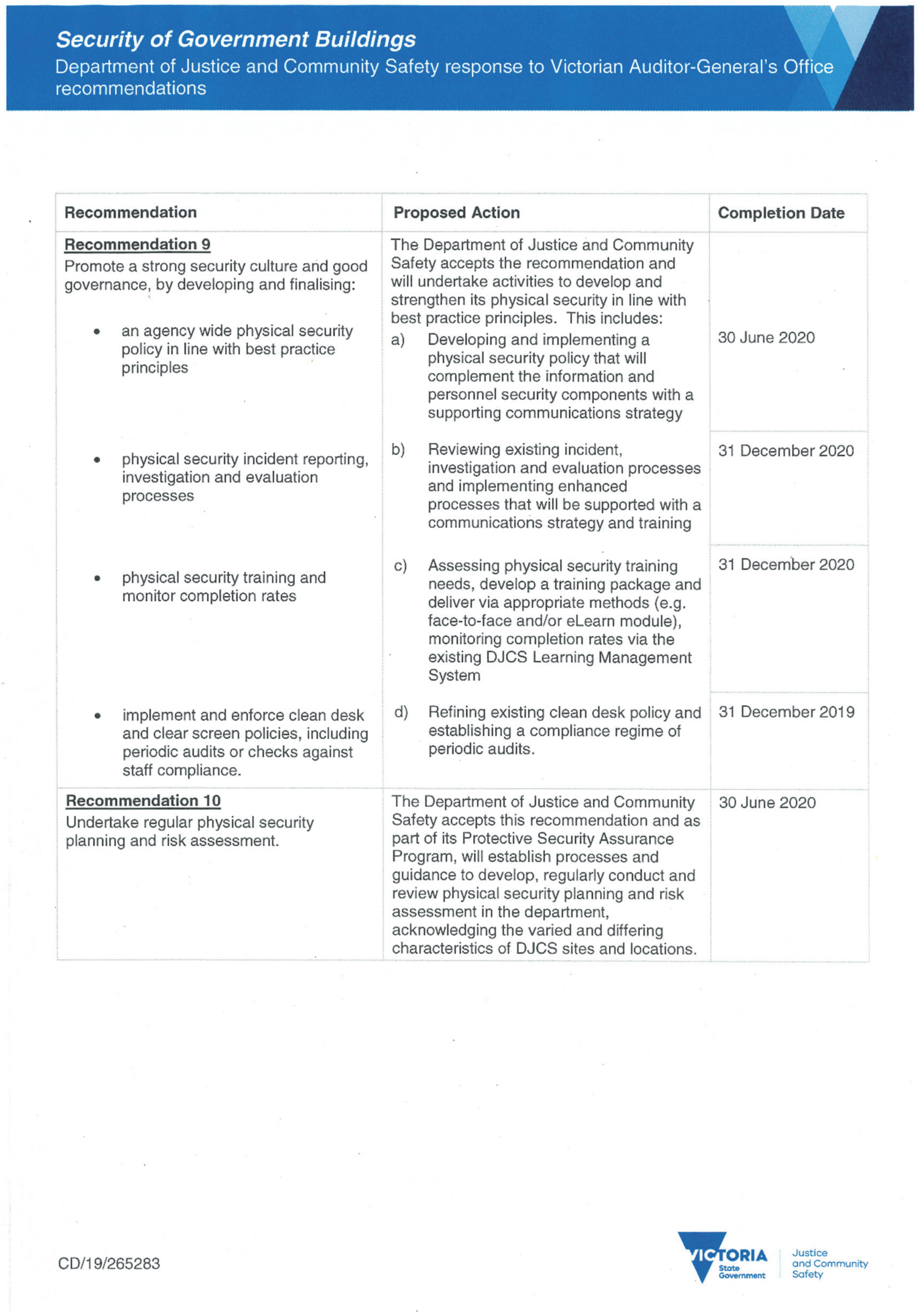
Rebecca Falkingham
Secretary

26 /4 /19

Personal and health information received by the Department of Justice and Community Safety is managed in accordance with the Victorian privacy legislation. A copy of the Department's privacy policy is available at www.justice.vic.gov.au. For Privacy enquiries, please telephone (03) 8684 0071.

Page 1 of 1

RESPONSE provided by the Secretary, DJCS—continued



Security of Government Buildings

Department of Justice and Community Safety response to Victorian Auditor-General's Office recommendations

Recommendation	Proposed Action	Completion Date
Recommendation 9 Promote a strong security culture and good governance, by developing and finalising: • an agency wide physical security policy in line with best practice principles	The Department of Justice and Community Safety accepts the recommendation and will undertake activities to develop and strengthen its physical security in line with best practice principles. This includes: a) Developing and implementing a physical security policy that will complement the information and personnel security components with a supporting communications strategy	30 June 2020
• physical security incident reporting, investigation and evaluation processes	b) Reviewing existing incident, investigation and evaluation processes and implementing enhanced processes that will be supported with a communications strategy and training	31 December 2020
• physical security training and monitor completion rates	c) Assessing physical security training needs, develop a training package and deliver via appropriate methods (e.g. face-to-face and/or eLearn module), monitoring completion rates via the existing DJCS Learning Management System	31 December 2020
• implement and enforce clean desk and clear screen policies, including periodic audits or checks against staff compliance.	d) Refining existing clean desk policy and establishing a compliance regime of periodic audits.	31 December 2019
Recommendation 10 Undertake regular physical security planning and risk assessment.	The Department of Justice and Community Safety accepts this recommendation and as part of its Protective Security Assurance Program, will establish processes and guidance to develop, regularly conduct and review physical security planning and risk assessment in the department, acknowledging the varied and differing characteristics of DJCS sites and locations.	30 June 2020

CD/19/265283

VICTORIA State Government | Justice and Community Safety

Auditor-General’s reports tabled during 2018–19

Report title	Date tabled
Local Government Insurance Risks (2018–19:1)	July 2018
Managing the Municipal and Industrial Landfill Levy (2018–19:2)	July 2018
School Councils in Government Schools (2018–19:3)	July 2018
Managing Rehabilitation Services in Youth Detention (2018–19:4)	August 2018
Police Management of Property and Exhibits (2018–19:5)	September 2018
Crime Data (2018–19:6)	September 2018
Follow up of Oversight and Accountability of Committees of Management (2018–19:7)	September 2018
Delivering Local Government Services (2018–19:8)	September 2018
Security and Privacy of Surveillance Technologies in Public Places (2018–19:9)	September 2018
Managing the Environmental Impacts of Domestic Wastewater (2018–19:10)	September 2018
Contract Management Capability in DHHS: Service Agreements (2018–19:11)	September 2018
State Purchase Contracts (2018–19:12)	September 2018
Auditor-General’s Report on the Annual Financial Report of the State of Victoria: 2017–18 (2018–19:13)	October 2018
Results of 2017–18 Audits: Local Government (2018–19:14)	December 2018
Professional Learning for School Teachers (2018–19:15)	February 2019
Access to Mental Health Services (2018–19:16)	March 2019
Outcomes of Investing in Regional Victoria (2018–19:17)	May 2019
Reporting on Local Government Performance (2018–19:18)	May 2019
Local Government Assets: Asset Management and Compliance (2018–19:19)	May 2019
Compliance with the Asset Management Accountability Framework (2018–19:20)	May 2019

VAGO

Victorian Auditor-General's Office

All reports are available for download in PDF and HTML format on our website
www.audit.vic.gov.au

Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne Vic 3000
AUSTRALIA

Phone +61 3 8601 7000
Email enquiries@audit.vic.gov.au