The Auditor-General
Audit Report No.49 2013–14
Performance Audit

The Management of Physical Security

Australian Crime Commission

Geoscience Australia

Royal Australian Mint

Australian National Audit Office

ISSN 1036–7632
ISBN 0 642 81488 0 (Print)
ISBN 0 642 81489 9 (Online)

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
publications@anao.gov.au.

Australian National
Audit Office

Canberra ACT
24 June 2014

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Australian Crime Commission, Geoscience Australia and the Royal Australian Mint titled *The Management of Physical Security.* The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7505
Fax: (02) 6203 7519
Email: publications@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:

http://www.anao.gov.au

Audit Team

William Bonney
Denis Preston
Donna Burton

Contents

Abbreviations ... 7
Glossary ... 8

Summary and Recommendations ... 9

Summary ... 11
- Introduction ... 11
- Audit objective, criteria and scope ... 14
- Overall conclusion ... 15
- Key findings by chapter ... 18
- Summary of agency responses ... 21

Recommendations ... 23

Audit Findings ... 25

1. Introduction ... 27
   - Introduction ... 27
   - Audit objective and criteria ... 32
   - Audit approach ... 33
   - Structure of this report ... 35
2. Governance Arrangements ... 36
   - Introduction ... 36
   - Roles and responsibilities ... 37
   - Monitoring and reporting ... 39
   - Information sharing and collaboration ... 44
   - Assessment of compliance with mandatory requirements and implementation of previous ANAO recommendations ... 45
   - Conclusion ... 47
3. Security Risk Management ... 49
   - Introduction ... 49
   - Approach and methodology ... 50
   - Links with policies and plans ... 55
   - Assessment of compliance with mandatory requirements and implementation of previous ANAO recommendations ... 57
   - Conclusion ... 59
4. Control Activities ... 61
   - Introduction ... 61
   - Management of security documentation ... 61
   - Security procedures in practice ... 63
   - Training and awareness ... 64
   - Assessment of compliance with mandatory requirements and implementation of previous ANAO recommendations ... 69
   - Conclusion ... 69

Appendices 71
Appendix 1: Agency responses 73
Appendix 2: Protective security principles 76
Appendix 3: PSPF mandatory requirements 78
Appendix 4: Further analysis of the reported levels of agencies' self-assessed compliance with the 16 mandatory requirements examined in this audit 81
Index 83

Tables

Table S.1: Overview of the agencies in this audit 13
Table 1.1: Relevant previous audit recommendations 30
Table 1.2: Overview of the agencies in this audit 32
Table 1.3: ANAO assessment rating system 34
Table 2.1: PSPF prescribed security roles 37
Table 2.2: Self-assessment compliance reported by the audited agencies 41
Table 2.3: Assessment against mandatory requirements 46
Table 2.4: Implementation of previous ANAO recommendation 47
Table 3.1: Broad elements of security risk management 50
Table 3.2: Agencies' security risk assessment practices against key aspects prescribed in the PSPF 53
Table 3.3: Assessment against mandatory requirements 57
Table 3.4: Implementation of previous ANAO recommendations 59
Table 4.1: Key security documents observed at the audited agencies 63
Table 4.2: Key security awareness training program completion statistics 66
Table 4.3: Assessment against mandatory requirements 69
Table 4.4: Implementation of previous ANAO recommendations 69
Table A.1: PSPF mandatory requirements in scope for this audit 78

Figures

Figure 2.1: Reported compliance and non-compliance by mandatory requirement 43
Figure 4.1: Channels for promoting security awareness 65
Figure A.1: Reported compliance by agency size 81
Figure A.2: Reported compliance by agency group 82

Abbreviations

ACC	Australian Crime Commission
AGD	Attorney-General's Department
ANAO	Australian National Audit Office
ASA	Agency Security Adviser
ASE	Agency Security Executive
CAC Act	*Commonwealth Authorities and Companies Act 1997*
FMA Act	*Financial Management and Accountability Act 1997*
GA	Geoscience Australia
ICT	information and communications technology
ITSA	Information Technology Security Adviser
Mint	Royal Australian Mint
PGPA	*Public Governance, Performance and Accountability Act 2013*
PSM	Protective Security Manual
PSPF	Protective Security Policy Framework

Glossary

Agency Security Adviser	The person responsible for the day-to-day protective security functions within an agency.
Agency Security Executive	The Senior Executive Service officer (or equivalent) responsible for oversighting an agency's protective security policies and practices.
Information security	The policies and practices used to protect an agency's records, documents and data. A subset of information security—information and communications technology security—is concerned with the protection of electronic information and systems.
Information Technology Security Adviser	The person responsible for advising senior management on information and communications technology security-related functions.
Personnel security	The policies and practices designed to assess and manage the continued eligibility and suitability of those individuals requiring access to sensitive or security classified information and resources.
Physical security	The policies and practices designed to prevent the loss of, or unauthorised access to, an agency's official resources; and help maintain a safe and secure working environment for staff, contracted service providers and members of the public.
Protective security	The collective term for the broad set of policies and practices employed to protect the Australian Government's official information, assets, and people.

Summary and Recommendations

Summary

Introduction

1. Effective protective security can help maintain the operating environment necessary for the confident and secure conduct of government business, the delivery of government services and the achievement of policy outcomes. Well-designed protective security arrangements can support Australian Government agencies to manage risks and threats that could result in: harm to their staff or to members of the public; the compromise or loss of official information or assets; or not achieving the Government's policy objectives.[1]

Protective Security Policy Framework

2. Protective security in Australian Government agencies is governed by the *Protective Security Policy Framework* (PSPF), which adopts a principles-based approach[2] to protective security. Under the PSPF, relevant agencies[3] are required to establish appropriate protective security arrangements to mitigate threats or attacks against people, information or assets based on an assessment of their particular security risks and threats.

3. The PSPF considers physical security to be a combination of physical and procedural measures that should provide a safe and secure environment for the agency's employees, contracted service providers, members of the

[1] Based on Attorney-General's Department, *Overarching protective security policy statement*, located at: <http://www.protectivesecurity.gov.au/pspf/Pages/Overarching-protective-security-policy-statement.aspx> [Date accessed: 30 April 2014].

[2] The protective security principles are shown in Appendix 2. The earlier Protective Security Manual (PSM) adopted a more compliance-based approach.

[3] The PSPF applies to all *Financial Management and Accountability Act 1997* (FMA Act) agencies, and to those *Commonwealth Authorities and Companies Act 1997* (CAC Act) bodies that have received a Ministerial Direction. This arrangement is currently being reviewed following the passage of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), which, at the time of preparation of this report, is planned to take effect on 1 July 2014 and replace the FMA and CAC Acts. The PGPA Act removes the distinction between FMA Act agencies and CAC Act bodies, and introduces two broad categories of Australian Government entities (non-corporate and corporate Commonwealth entities) and the category of Commonwealth companies. Under section 21 of the PGPA Act, non-corporate Commonwealth entities must be governed in a way that is not inconsistent with the policies of the Australian Government, including the PSPF, whereas corporate Commonwealth entities and Commonwealth companies do not have to apply Australian Government policies, including the PSPF, unless the Finance Minister issues a *Government Policy Order* under sections 22 or 93 of the Act.

public, and agency resources. According to the PSPF, an agency's physical security program should aim to:

- Deter—measures implemented which adversaries perceive as too difficult, or needing special tools and training to defeat.
- Detect—measures implemented to determine if an unauthorised action is occurring or has occurred.
- Delay—measures implemented to:
  - impede an adversary during an attack, or
  - slow the progress of a detrimental event to allow a response before agency information or physical assets are compromised.
- Respond—measures taken once an agency is aware of an attack or event to prevent, resist or mitigate the attack or event.
- Recover—measures taken to restore operations to normal (as far as possible) following an incident.[4]

4. An agency's protective security policies, plans and procedures—which typically comprise a mix of governance, personnel security, information security, and physical security components—should be integrated into the agency's day-to-day operations and management activities.

5. In 2013, agencies were required to undertake a self-assessment of, and to report on, their compliance with the PSPF's 33 mandatory requirements.[5] These arrangements were introduced following a two year implementation period intended to allow sufficient time for agencies to adopt the new protective security (including physical security) requirements.

Selected agencies in this audit

6. Three agencies were selected by the Australian National Audit Office (ANAO) to be included in this performance audit: the Australian Crime Commission (ACC); Geoscience Australia (GA); and the Royal Australian Mint

[4] Attorney-General's Department, *Physical security management protocol*, July 2011, p.1, available at: <http://www.protectivesecurity.gov.au/physicalsecurity/Documents/PHYSEC%20Protocol%20-%20V1.4%20-%20as%20approved%2018%20July%202011%20-%20amended%20July%202013.pdf>. [Date accessed: 23 August 2013].

[5] Agencies were required to report their compliance with the PSPF's mandatory requirements to their portfolio Minister, the Secretary of the Attorney-General's Department and the Auditor-General.

(Mint). The selected agencies each face a range of physical security risks arising from their organisational objectives and operations, and the characteristics and sensitivity of the information and assets in their care. Further information on these agencies' physical security risk context and operating environment is provided in Table S.1.

Table S.1: Overview of the agencies in this audit

	ACC	GA	Mint
Overview	Provides intelligence, investigation and criminal database services and has a role in combating serious and organised crime in Australia.	Australia's national geoscience[A] agency—provides advice to the Australian Government, industry and other stakeholders.	Produces coins, medals, medallions, tokens and seals for national and international clients, including other governments.
Number of staff	630	700	210
Number of sites	8	2	2
Annual number of public visitors	N/A	16 000	200 000
Physical risk focus	The protection of: sensitive and classified information and intelligence; the Commission's premises and property, including specialised surveillance equipment; ACC staff and witnesses; and also members of the public that interact with the Commission's functions.	The protection of: sensitive geospatial information; specialised sensory equipment and physical collections; GA's premises and staff, as well as visitors to GA, including school students.	The protection of: designs used for production of coins and medals; stocks of precious metals and coins; specialised engineering and manufacturing equipment; the Mint's staff; and members of the public who visit the Mint.

Source: Based on information at the selected agencies.

Note A: Any sciences relating to the earth.

Audit objective, criteria and scope

7. The audit objective was to assess the effectiveness of physical security arrangements in selected Australian Government agencies, including whether applicable Australian Government requirements are being met.

8. To form a conclusion against the objective, the ANAO adopted the following high-level criteria:

- appropriate protective security governance arrangements are in place, including clear roles and responsibilities and sound arrangements for training, communication, incident management and reporting;
- a sound physical security risk assessment was undertaken and suitable management practices were established; and
- a physical security policy and an agency security plan have been developed and implemented, and are supported by relevant procedures.

9. The audit assessed the selected agencies' management of physical security against: the seven mandatory PSPF requirements for physical security; and nine of the 13 mandatory PSPF governance[6] requirements. Appendix 3 provides details of the 16 PSPF mandatory requirements addressed in this audit. The audit did not assess the selected agencies against the PSPF mandatory requirements relating to information security and personnel security, or the information and communications technology (ICT) security requirements contained in the *Information Security Manual*.[7] A forthcoming ANAO performance audit will examine the application of ICT security requirements relating to cyber-security by seven Australian Government agencies.[8]

10. Further, the Attorney-General's Department's (AGD) policy and coordination role was not examined in this audit. However, where the ANAO

[6] The term 'governance' is used in the PSPF to describe the group of mandatory requirements designed to help ensure that agencies have the foundation elements necessary to meet the Government's protective security policy standards and expectations. The four governance requirements not addressed in the audit were GOV 9, GOV 10, GOV 11 and GOV 13 as they relate, respectively, to: providing guidance to employees and contractors on certain sections from the *Crimes Act 1914*, the *Criminal Code 1995*, the *Freedom of Information Act 1982* and the *Privacy Act 1988;* compliance with multilateral or bilateral agreements; business continuity management; and fraud control.

[7] The *Information Security Manual* (ISM) produced by the Australian Signals Directorate (ASD) is the standard which governs the security of government ICT systems. The ISM is available from <http://www.asd.gov.au/infosec/ism/index.htm>. [Date accessed: 19 May 2014].

[8] ANAO, Audit Report No.50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems*.

identified matters that may affect implementation of the physical security requirements at a whole-of-government level, they are discussed in this report.

11. The audit did, however, examine whether the selected agencies had implemented a number of recommendations made in earlier ANAO across-agency performance audits that addressed matters relevant to the management of physical security, namely: Audit Report No.23 2002–03, *Physical Security Arrangements in Commonwealth Agencies*; and Audit Report No.25 2009–10, *Security Awareness and Training*.[9]

Overall conclusion

12. The protection of sensitive information, agency resources and staff is an ongoing responsibility of Australian Government agencies. Under the mandatory requirements set out in the PSPF, agencies must provide and maintain a safe working environment for their staff, contractors, and members of the public and limit the potential for compromise of the confidentiality, integrity and availability of official information and assets.[10] Agencies are expected to manage foreseeable security risks, having regard to their business context and operations, within available resources.

13. The agencies selected for this audit—the Australian Crime Commission (ACC), Geoscience Australia (GA), and the Royal Australian Mint (Mint)—each experience a range of physical security risks, threats and challenges in the conduct of their business activities, reflecting their particular mix of functions, assets and information holdings.

14. Overall, the physical security arrangements adopted by each of the selected agencies were generally effective, and for the most part, the agencies had met, or partially met, the applicable PSPF requirements. Key physical security controls and procedures tested by the ANAO in each agency were largely aligned with the agencies' identified risks and specific business needs, and were generally operating as intended. Nonetheless, there were areas where improvements were warranted; most notably, there was scope to better align security risk management activities with the PSPF's requirements, including identifying and managing risks to the public, and further integrating security

[9] See Table 1.1 for a listing of the previous ANAO recommendations examined in this audit.

[10] Attorney-General's Department, *Protective Security Policy Framework*, June 2013, p.2, available at: <http://www.protectivesecurity.gov.au/pspf/Documents/Protective%20Security%20Policy%20Framework%20-%20amended%20June%202013.pdf>. [Date accessed: 23 August 2013].

risks with other organisational risk activities. There were also opportunities to improve the ongoing effectiveness of physical security management by adopting a more structured approach to security assurance and monitoring arrangements; a process which benefits from senior leadership oversight.

15. Observations on the key areas of the audit's focus are discussed in the following paragraphs. The key areas relate to: governance; security risk management; security controls and procedures; compliance with selected PSPF mandatory requirements; and the implementation of relevant recommendations made in previous ANAO performance audits.

16. Each agency established appropriate governance arrangements to oversee the management of physical security, including appointing appropriately skilled and experienced staff to key security roles. In addition, the Mint had established appropriate security assurance and monitoring arrangements—providing a sound basis for assessing the ongoing effectiveness of its policies and control measures relative to its evolving risk environment.

17. The Mint was the only agency that had consistently implemented the full range of security risk management processes, as part of the risk-based approach to physical security required by the PSPF. The approach adopted by the Mint included consideration of risks relating to the duty of care owed to members of the public. At the ACC and GA, opportunities were identified to: bring the conduct of security risk assessments into line with the requirements of the PSPF; improve linkages between their security risk activities and other agency risk management activities; and better demonstrate how their security policies and underlying procedures aligned with their assessed security risks.

18. Key controls identified by agencies in their security-related policies and procedures that were examined by the ANAO were generally operating as intended. Further, the ANAO did not identify any significant gaps in the security control environment for any of the three agencies. The three agencies had also established processes to promote an effective security risk culture, including raising awareness of security issues through the implementation of training and other information and communication measures.

19. The ANAO's assessment of the agencies' compliance with the PSPF mandatory requirements relevant to this audit was broadly consistent with the agencies' self-assessments.[11] Overall, the level of compliance assessed for the agencies reflects a level of maturity with the risk-based approach required under the PSPF that might be expected at this relatively early stage of the PSPF's application.

20. The ACC and Mint had taken appropriate steps to address past ANAO audit recommendations relating to physical security. However, GA was assessed as having not implemented one of the recommendations and only partially implemented a number of the recommendations.

21. This audit has highlighted some key lessons for senior leaders as agencies continue to work towards implementation of the physical security requirements and standards prescribed by the PSPF. Agency security is a shared responsibility, which requires security awareness and accountability at all levels. A strong internal security culture is enhanced by integrating the assessment and ongoing management of security risks into an agency's governance and enterprise-wide risk management arrangements. Periodic executive review of an agency's physical security risks and posture, including by boards of management, can provide added oversight and assurance that risks have been managed appropriately.

22. The ANAO has made two recommendations directed at strengthening the design and application of physical security assurance and monitoring activities, and security risk management practices. It is important that all Australian Government agencies actively monitor their protective security risks—and the effectiveness of controls designed to mitigate those risks—in light of their changing operational contexts and the constrained resourcing environment facing agencies. The recommendations have broad applicability to other Australian Government agencies.

[11] The ANAO downgraded the agencies' self-assessment ratings in 14 instances—in one case at GA the ANAO considered the agency's self-assessment rating of 'compliant' to be 'non-compliant', in 12 cases (nine at the ACC and three at GA) the ANAO considered ratings of 'compliant' to be 'partially compliant' and in one case at GA, the ANAO considered a rating of 'partially compliant' to be 'non-compliant'. The ANAO also upgraded one self-assessment rating at GA—from 'partially compliant' to 'compliant'—to reflect improvements made by GA since September 2013.

Key findings by chapter

Governance Arrangements (Chapter 2)

23. Protective security governance, as set out in the PSPF[12], involves both *conformance*—how an agency uses protective security arrangements to ensure it meets its obligations and Government expectations—and *performance*—how an agency uses protective security arrangements to contribute to its overall performance.

24. Sound arrangements for the delivery and oversight of physical security activities were in place at each of the selected agencies. Specifically, each of the agencies had clearly identified the key security roles and responsibilities required by the PSPF.[13] At each agency, the personnel appointed to these roles possessed an appropriate level of knowledge, skills and experience[14], enabling them to fulfil their duties. Importantly, all agencies had established forums to oversee and support the management of physical security. The Mint and GA had established dedicated security committees, while the ACC had a broader-focused operational management committee where security related matters could be raised.

25. To assist in monitoring both the performance and conformance aspects of the PSPF, agencies should establish a security assurance strategy outlining their approach to managing protective security. An assurance strategy is an important means to guide approaches to monitoring the ongoing effectiveness of agencies' security policies and control measures relative to an evolving risk environment. The Mint had defined a security assurance strategy, outlining its approach to the oversight and monitoring of security requirements. At an operational level, however, all agencies had processes and procedures to identify and resolve day-to-day physical security incidents.

26. Each of the audited agencies submitted their first self-assessment compliance report against the PSPF's mandatory requirements to the AGD in September 2013, as required.[15] In doing so, the ACC and GA adopted a three-level rating system—'compliant', 'partially compliant' or 'non-compliant'. However, this approach was inconsistent with the reporting guidance in the

[12] AGD, PSPF, op. cit., p. 3.

[13] PSPF mandatory requirement GOV 2.

[14] PSPF mandatory requirement GOV 3.

[15] PSPF mandatory requirement GOV 7.

PSPF.[16] Specifically, the guidance proposes that the status of each mandatory requirement be reported as 'fully compliant', 'non-compliant' or 'not applicable'. In cases of non-compliance, the guidance suggests that further details—such as mitigation measures and residual risks—should also be supplied.

27. The ANAO observed that the binary (fully compliant or non-compliant) approach proposed by the AGD does not adequately reflect circumstances where agencies may have met most aspects of a particular requirement, but have outstanding actions (at the time of preparing their report) to demonstrate full compliance. Further, it does not capture agencies' progress as they work towards an improved level of compliance. In the course of this audit, AGD advised that it plans to develop additional guidance material for agencies' self-assessment and reporting, and are also investigating the potential of using a 'maturity level model' for PSPF reporting.

28. The PSPF reinforces the importance of having strong communication channels within an agency—including alignment between protective security and work health and safety and giving consideration to security issues during the design or modification of facilities.[17] The PSPF also suggests agencies share information or collaborate with other agencies in relation to security management. The Mint had structured arrangements in place to support ongoing communication and collaboration between the security team and key internal stakeholders—including 'health and safety' staff—and other government agencies. Equivalent arrangements in the ACC and GA were mostly informal and the agencies were unable to demonstrate that these arrangements were consistently applied.

Risk Management (Chapter 3)

29. Under the PSPF, agencies are required to adopt a risk-based approach to managing protective security, including physical security.[18] While each of the agencies had formal enterprise-wide risk management policies and procedures, the Mint had also clearly defined its approach to, and methodology for, the management of security risks.

[16] AGD, *Protective Security Governance Guidelines: Compliance Reporting*, March 2012, pp. 10–11.

[17] PSPF mandatory requirements PHYSEC 3 and PHYSEC 4.

[18] PSPF mandatory requirement GOV 6.

30. Each agency had recently conducted an assessment of security risks and associated treatment options. The Mint was the only agency that had consistently implemented the full range of security-specific risk management practices required by the PSPF[19], being the: identification of critical assets; assessment of business impact levels; assessment of risks to the public; identification of site-specific risks and development of associated plans; and assessment for heightened threat levels. The ACC and GA had established some of these measures but not all, or had not applied them on a consistent basis.

31. Further, the Mint demonstrated that it had an integrated approach to aligning security risk management activities with other organisational risk activities, such as fraud control planning. An integrated approach facilitates internal understanding and assessment of the interdependencies between security risks and other risks.

32. The PSPF provides that agencies should develop protective security policies and plans to meet business needs commensurate with the nature and assessment of identified risks.[20] The Mint was able to demonstrate that its security policies and plans had been updated and aligned to the outcomes of their most recent security risk assessment. Both the ACC and GA advised that they were in the process of doing so—having finalised their protective security risk assessments in January 2013 and June 2012 respectively.

Control Activities (Chapter 4)

33. To effectively manage their physical security risks and threats, agencies will typically have in place a range of measures, processes or controls. Staff are more likely to understand the nature and purpose of these controls, including their responsibilities for the day-to-day operation of these measures, where agencies have appropriately tailored procedural documentation, and well-designed security awareness and training mechanisms.

34. The ANAO's examination of a selection of the procedures and controls implemented to manage key physical security risks at each of the audited agencies, found that the controls were generally operating as intended. Importantly, the observed controls generally aligned with each agency's security policies, plans and procedural documentation.

[19] PSPF mandatory requirements GOV 6, PHYSEC 5 and PHYSEC 7.

[20] PSPF mandatory requirements GOV 4, GOV 5 and PHYSEC 1.

35. Providing staff and contractors with security awareness training tailored to the agency's operating circumstances and risks reinforces understanding of security-related responsibilities, and also supports promotion and maintenance of a security-aware culture.[21] The agencies had each established suitable security training and awareness programs using a range of communication methods and delivery channels. In each agency, the components of awareness and training programs that were examined during the audit were mandatory for all staff and incorporated content that was well-designed and informative. Notably, the content of each component of the security awareness training programs examined by the ANAO was consistent with the nature of each agency's security context. At GA and the Mint, service providers were also required to complete the security awareness training. Overall, completion rates of the security awareness training at the three agencies were generally high.[22] The agencies advised that they had taken steps to address the issue of some staff not completing the training.

Summary of agency responses

36. The proposed audit report was provided to each of the audited agencies, and an extract of the proposed report was provided to AGD. Each agency's formal response to the proposed report is included at Appendix 1.

37. In addition, AGD provided the following summary comments:

> The Attorney-General's Department (AGD) has protective security policy responsibility for the Australian Government as detailed in the Protective Security Policy Framework (PSPF). AGD supports the two recommendations which will strengthen the risk management approach to protective security within agencies, while providing assurance that the measures implemented remain effective.
>
> An agency's PSPF compliance report requires qualification where compliance with the mandatory requirement is not met. The primary focus of this qualification is to identify the residual risks the agency is exposed to, and how the agency plans to mitigate those risks and achieve compliance with the mandatory requirement over time. AGD considers that reporting 'partial compliance', as a degree of non-compliance with a mandatory requirement, is

[21] PSPF mandatory requirement GOV 1.

[22] Completion rates of security awareness training at the Mint, GA and at the ACC were 98 per cent, 96 per cent and 87 per cent respectively.

unnecessary as this distinction can be made as a part of the agency's qualification.

Recommendations

The recommendations are based on the findings from fieldwork at the selected agencies, but are likely to be relevant to other Australian Government agencies. Therefore, all agencies are encouraged to assess the benefits of implementing the recommendations in light of their own circumstances.

Recommendation No.1

Paragraph 2.15

To strengthen security assurance and monitoring arrangements, the ANAO recommends that agencies implement a security assurance strategy that outlines their approach to monitoring:

- compliance with the PSPF and the agency's security policies; and
- the ongoing effectiveness of the agency's security policies and control measures.

ACC's response: *Agree*.

AGD's response: *Supported*.

GA's response: *Accepted*.

Mint's response: *Agree*.

Recommendation No.2

Paragraph 3.25

To assist agencies to adopt and maintain an effective approach to the management of physical security risks, the ANAO recommends that agencies, in the context of their discrete operating circumstances:

- integrate security risk management activities with other organisational risk activities;
- tailor procedures for the conduct of security risk assessments that align to the requirements of the PSPF; and
- update security policies and plans to reflect the outcomes of security risk assessments.

ACC's response: *Agree*.

AGD's response: *Supported*.

GA's response: *Accepted*.

Mint's response: *Agree*.

Audit Findings

1. Introduction

This chapter provides an overview of the Australian Government's framework for the management of physical security. It also outlines the agencies selected for examination and the audit objective, scope and approach.

Introduction

1.1 Effective protective security can help maintain the operating environment necessary for the confident and secure conduct of government business, the delivery of the Australian Government's services and achievement of policy outcomes. Well-designed protective security arrangements can support agencies to manage the risks and threats that could result in: harm to their staff or to members of the public; the compromise or loss of official information or assets; or not achieving the Government's objectives.[23]

1.2 An agency's protective security policies, plans and procedures—which typically comprise a mix of governance, personnel security, information security, and physical security components—should be integrated into the agency's day-to-day operations and management activities.

Protective Security Policy Framework

1.3 Protective security in Australian Government agencies is governed by the Protective Security Policy Framework (PSPF). Under the PSPF, relevant agencies are responsible for creating and maintaining appropriate protective security arrangements to mitigate threats against their people, information, or assets based on an assessment of their particular security risks and threats.

1.4 The PSPF adopts a principles-based[24] approach to protective security—the protective security principles contained in the PSPF are shown in Appendix 2. The PSPF was first introduced in June 2010 and applies to all *Financial Management and Accountability Act 1997* (FMA Act) agencies, and to those *Commonwealth Authorities and Companies Act 1997* (CAC Act) bodies that

[23] Based on Attorney-General's Department, *Overarching protective security policy statement*, located at: <http://www.protectivesecurity.gov.au/pspf/Pages/Overarching-protective-security-policy-statement.aspx>. [Date accessed: 30 April 2014].

[24] The earlier Protective Security Manual (PSM) adopted a more compliance-based approach.

have received a Ministerial Direction.[25] This arrangement is currently being reviewed following the passage of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), which, at the time of preparation of this report, is planned to take effect on 1 July 2014 and replace the FMA and CAC Acts.[26]

1.5 The PSPF contains the following 33 mandatory requirements relating to protective security:

- Governance[27]—13 mandatory requirements;
- Personnel security—6 mandatory requirements;
- Information security—7 mandatory requirements; and
- Physical security—7 mandatory requirements.

1.6 The 33 mandatory requirements outline the minimum standards that need to be considered and assessed for protective security management. Supporting the mandatory requirements are detailed protocols, standards and guidelines.

1.7 In 2013, agencies were required to undertake a self-assessment of, and to report on, their compliance with the PSPF's 33 mandatory requirements.[28] These arrangements were introduced following a two year implementation period intended to allow sufficient time for agencies to adopt the new protective security (including physical security) requirements.

[25] AGD advised the ANAO that to date, no CAC Act bodies have been issued with a direction to apply the PSPF. However, a number of CAC Act bodies have voluntarily adopted the mandatory requirements of the PSPF—as shown in footnote 44.

[26] The PGPA Act removes the distinction between FMA Act agencies and CAC Act bodies, and introduces two broad categories of Australian Government entities (non-corporate and corporate Commonwealth entities) and the category of Commonwealth companies. Under section 21 of the PGPA Act, non-corporate Commonwealth entities must be governed in a way that is not inconsistent with the policies of the Australian Government, including the PSPF, whereas corporate Commonwealth entities and Commonwealth companies do not have to apply Australian Government policies, including the PSPF, unless the Finance Minister issues a *Government Policy Order* under sections 22 or 93 of the Act.

[27] The term 'governance' is used in the PSPF to describe the group of mandatory requirements designed to help ensure that agencies have the foundation elements necessary to meet the Government's protective security policy standards and expectations.

[28] Agencies were required to report their compliance with the PSPF's mandatory requirements to their portfolio Minister, the Secretary of the Attorney-General's Department and the Auditor-General.

Physical security

1.8 The PSPF treats physical security as a combination of physical and procedural measures designed to provide a safe and secure environment for the agency's employees, contracted service providers, members of the public interacting with an agency, as well as the agency's official resources. According to the PSPF, an agency's physical security program should aim to:

- Deter—measures implemented which adversaries perceive as too difficult, or needing special tools and training to defeat.
- Detect—measures implemented to determine if an unauthorised action is occurring or has occurred.
- Delay—measures implemented to:
  - impede an adversary during an attack, or
  - slow the progress of a detrimental event to allow a response before agency information or physical assets are compromised.
- Respond—measures taken once an agency is aware of an attack or event to prevent, resist or mitigate the attack or event.
- Recover—measures taken to restore operations to normal (as far as possible) following an incident.[29]

1.9 Physical security arrangements should be designed to mitigate the broad range of the threats that an agency may face, including: civil unrest; unauthorised access or theft of agency or staff property; safety of agency staff or members of the public; acts of terrorism; and natural or industrial disasters.[30]

Previous audit activity

1.10 Since 2000, the Australian National Audit Office (ANAO) has conducted 12 across-agency performance audits of protective security arrangements in

[29] Attorney-General's Department, *Physical security management protocol*, July 2011, p.1, available at <http://www.protectivesecurity.gov.au/physicalsecurity/Documents/PHYSEC%20Protocol%20-%20V1.4%20-%20as%20approved%2018%20July%202011%20-%20amended%20July%202013.pdf>. [Date accessed: 23 August 2013].

[30] ibid.

Australian Government agencies.[31] A number of these audits have made recommendations related to physical security policy and practices. The relevant recommendations are outlined in Table 1.1.

Table 1.1: Relevant previous audit recommendations

Area	Recommendation	Source
Risk Assessments	Conduct comprehensive protective security risk assessments at least every three years as part of an agency-wide approach to risk management.	*Audit Report No.23 (2002–03) Recommendation No.1*
	Maintain documentation that supports agency decision-making processes for the prioritisation, selection and implementation of treatment options that address their identified security risks.	*Audit Report No.23 (2002–03) Recommendation No.2*
Education and Awareness	Develop and document comprehensive, consistent and logically referenced security plans and procedures. Develop and schedule periodic formal education and awareness programs for non-security personnel addressing agency security standards. In addition, agencies' security personnel and contractors should receive regular protective security and risk management training to ensure that they are sufficiently skilled to fulfil their responsibilities for security.	*Audit Report No.23 (2002–03) Recommendation No.3*
	Develop a security awareness and training plan that is commensurate with the organisation's circumstances, including its size and security risk profile.	*Audit Report No.25 (2009–10) Recommendation No.2*
	Tailor security awareness training programs to reflect the organisation's security risks and issues.	*Audit Report No.25 (2009–10) Recommendation No.3*
Physical Work Environment	Ensure the security risk assessment process, implemented security controls, and documented security procedures, adequately address all staff safety concerns.	*Audit Report No.23 (2002–03) Recommendation No.4*

[31] On 8 May 2014, the ANAO presented to the Parliament a performance audit report that examined the adequacy and effectiveness of the Australian Electoral Commission's implementation of recommendation No.8(b) in ANAO Audit Report No.28 2009–10, *The Australian Electoral Commission's Preparation for and Conduct of the 2007 Federal General Election.* That recommendation related to providing greater physical security over the transport and storage of completed ballot papers. See ANAO Audit Report No. 31 2013–14, *The Australian Electoral Commission's Storage and Transport of Completed Ballot Papers at the September 2013 Federal General Election*.

Area	Recommendation	Source
Protection of Security Classified Information	Ensure the security risk assessments, implemented security controls, and documented security procedures adequately address all requirements for the storage, handling and processing of any security classified Information.	*Audit Report No.23 (2002–03) Recommendation No.5*
Incident Reporting	Improve the procedures surrounding the reporting and recording of physical security incidents to ensure that all relevant information is captured in a timely manner, and used constructively to improve the security environment.	*Audit Report No.23 (2002–03) Recommendation No.6*

Source: ANAO.

Selected agencies in this audit

1.11 Three agencies were selected by the ANAO to be included in this performance audit: the Australian Crime Commission (ACC); Geoscience Australia (GA); and the Royal Australian Mint (Mint). The selected agencies each face a range of physical security risks arising from their organisational objectives and operations, and the characteristics and sensitivity of the information and assets in their care. Further information on these agencies' physical security risk context and operating environment is provided in Table 1.2.

Table 1.2: Overview of the agencies in this audit

	ACC	GA	Mint
Overview	Provides intelligence, investigation and criminal database services and has a role in combating serious and organised crime in Australia.	Australia's national geoscience[A] agency—provides advice to the Australian Government, industry and other stakeholders.	Produces coins, medals, medallions, tokens and seals for national and international clients, including other governments.
Number of staff	630	700	210
Number of sites	8	2	2
Annual number of public visitors	N/A	16 000	200 000
Physical risk focus	The protection of: sensitive and classified information and intelligence; the Commission's premises and property, including specialised surveillance equipment; ACC staff and witnesses; and also members of the public that interact with the Commission's functions.	The protection of: sensitive geospatial information; specialised sensory equipment and physical collections; GA's premises and staff, as well as visitors to GA, including school students.	The protection of: designs used for production of coins and medals; stocks of precious metals and coins; specialised engineering and manufacturing equipment; the Mint's staff; and members of the public who visit the Mint.

Source: Based on information collected at the ACC, GA and the Mint.

Note A: Any sciences relating to the earth.

Audit objective and criteria

1.12 The audit objective was to assess the effectiveness of physical security arrangements in the selected Australian Government agencies, including whether applicable Australian Government requirements are being met.

1.13 To form a conclusion against the objective, the ANAO adopted the following high-level criteria:

- appropriate protective security governance arrangements are in place, including clear roles and responsibilities and sound arrangements for training, communication, incident management and reporting;
- a sound physical security risk assessment was undertaken and suitable management practices were established; and

- a physical security policy and an agency security plan have been developed and implemented, and are supported by relevant procedures.

Audit approach

1.14 The audit assessed the selected agencies' management of physical security against: the seven mandatory requirements for physical security in the PSPF; and nine of the 13 mandatory PSPF governance[32] requirements. Appendix 3 outlines the 16 PSPF mandatory requirements addressed in this audit. An overview of the reported levels of self-assessed compliance or non-compliance with the governance and physical security mandatory requirements examined in this audit is contained in Chapter 2.[33]

1.15 The audit did not assess the selected agencies against the PSPF mandatory requirements relating to information security and personnel security, or the information and communications technology (ICT) security requirements contained in the *Information Security Manual*.[34] A forthcoming ANAO performance audit will examine the application of ICT security requirements relating to cyber-security by seven Australian Government agencies.[35]

1.16 The audit also examined whether the selected agencies had implemented the audit recommendations identified in Table 1.1.

1.17 Table 1.3 sets out the rating system that was used for the assessment of the selected agencies' adherence to the mandatory PSPF requirements and the implementation of the relevant ANAO recommendations.

[32] The four governance requirements not addressed in the audit were GOV 9, GOV 10, GOV 11 and GOV 13 as they relate, respectively, to: providing guidance to employees and contractors on certain sections from the *Crimes Act 1914*, the *Criminal Code 1995*, the *Freedom of Information Act 1982* and the *Privacy Act 1988;* compliance with multilateral or bilateral agreements; business continuity management; and fraud control.

[33] Appendix 4 contains further analysis of the reported level of agencies' self-assessed compliance or non-compliance with the 16 mandatory requirements examined in this audit. Figure A.1 shows the level of compliance and non-compliance by agency size; and Figure A.2 shows the level of compliance and non-compliance by agency group.

[34] The *Information Security Manual* (ISM) produced by the Australian Signals Directorate (ASD) is the standard which governs the security of government ICT systems. The ISM is available from <http://www.asd.gov.au/infosec/ism/index.htm>. [Date accessed: 19 May 2014].

[35] ANAO, Audit Report No.50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems.*

Table 1.3: ANAO assessment rating system

Adherence to the PSPF mandatory requirements	Implementation of ANAO recommendations	Explanation
Compliant	Implemented	The agency demonstrated it had implemented the necessary actions for the PSPF mandatory requirements or met the intent of the recommendation.
Partially compliant	Partially implemented	This category encompassed two considerations: • the agency established a process or procedure to address the issue, however the specific action required by the PSPF mandatory requirement or the recommendation was not complete at the time of the ANAO's assessment; or • action taken either fell short of the intent of the PSPF mandatory requirement or the recommendation, or only addressed some of the outcomes.
Non-compliant	Not implemented	This category encompassed two considerations: • the action taken did not address the PSPF mandatory requirement or the recommendation; or • there was no supporting evidence that action had been undertaken.

Source: ANAO.

1.18 AGD's policy and coordination role was not examined in this audit. However, where the ANAO identified matters that may affect implementation of the physical security requirements at a whole-of-government level, they are discussed in this report.

1.19 The audit was conducted[36] in accordance with the ANAO's auditing standards at a cost to the ANAO of approximately $353 500.

[36] The ANAO engaged KPMG to deliver audit services as part of the conduct of this audit.

Structure of this report

1.20 Table 1.4 outlines the structure of the discussion of the audit findings and conclusions contained in this report.

Table 1.4: Structure of the report

Chapter 2	Chapter 2 discusses the results of the ANAO's examination of the selected agencies' protective security governance arrangements.
Chapter 3	Chapter 3 discusses the results of the ANAO's examination of the selected agencies' security risk management arrangements.
Chapter 4	Chapter 4 discusses the results of the ANAO's examination of the selected agencies' security control activities.

Source: ANAO.

2. Governance Arrangements

This chapter discusses the results of the ANAO's examination of the selected agencies' protective security governance arrangements.

Introduction

2.1 The PSPF reinforces the importance of having strong governance arrangements and practices to provide appropriate oversight and management of protective security—including physical security—arrangements. As outlined in the PSPF, good protective security governance entails:

> Conformance—how an agency uses protective security arrangements to ensure it meets the obligations of policy and standards and Government's expectations; and
>
> Performance—how an agency uses protective security arrangements to contribute to its overall performance through the secure delivery of goods, services or programmes as well as ensuring the confidentiality, integrity and availability of its people, information and assets. [37]

2.2 Specifically, the PSPF details the following principles for governance in the context of protective security[38]:

- accountability—being answerable for decisions and having meaningful mechanisms in place to help adherence to applicable protective security requirements and standards;
- transparency—having clear roles and responsibilities for protective security functions and clear procedures to support decision-making;
- efficiency—ensuring the best use of protective security-related resources in the context of supporting the achievement of the agency's objectives; and
- leadership—having broad commitment to good protective security performance driven by leadership from the top.

[37] Attorney-General's Department, *Protective Security Policy Framework*, June 2013, p.3, available at <http://www.protectivesecurity.gov.au/pspf/Documents/Protective%20Security%20Policy%20Framework%20-%20amended%20June%202013.pdf>. [Date accessed: 23 August 2013].

[38] ibid.

2.3 In evaluating governance arrangements the ANAO considered the following matters in this chapter:

- roles and responsibilities—roles and responsibilities to support effective physical security management are established, including appropriate governance arrangements;
- monitoring and reporting—the agencies have:
  - defined a formal security assurance strategy;
  - processes for managing security incidents; and
  - arrangements for providing appropriate levels of information about physical security activities to key internal stakeholders and to the AGD.[39]
- information sharing and collaboration—mechanisms and channels have been established to promote regular discussions around security matters.

Roles and responsibilities

2.4 The PSPF prescribes the key security roles that must be appointed in assisting agencies to meet their security obligations. Establishing key protective security roles and clearly defining their responsibilities provides a source of expertise and aids transparency and accountability.

2.5 The key security roles outlined in the PSPF are summarised in Table 2.1.

Table 2.1: PSPF prescribed security roles

Role	Security obligations
Agency Security Executive (ASE)	A member of the Senior Executive Service responsible for the oversight of agency protective security policy and practices.
Agency Security Adviser (ASA)	Responsible for the day-to-day performance of protective security functions.
Information Technology Security Adviser (ITSA)	Responsible for advising senior management on the security of the agency's information and communications technology (ICT) systems.

Source: *Protective Security Policy Framework: Securing Government Business 2010*, p.10.

[39] The agencies' approaches to monitoring physical security risks and activities are examined in Chapter 3 of this report.

Key security personnel

2.6 Each of the agencies had identified the key security roles and responsibilities shown in Table 2.1. In each case, the personnel appointed to these roles possessed appropriate skills, experiences and qualifications to fulfil their duties. Further, in all cases, the security responsibilities and obligations of these positions were clearly identified in key security documents.

2.7 The ASA in each of the three agencies was active in establishing and promoting the agencies' physical security framework and able to demonstrate an awareness of their agency's physical security environment. Further, the ASA in each of the selected agencies undertook, or managed other staff undertaking, the key functions outlined in the PSPF[40] that were in the scope of this audit.

Security committees

2.8 Agencies should establish formal governance structures to provide oversight over protective security arrangements, including physical security.

2.9 All of the audited agencies had established governance committees that provided, to varying degrees, a forum for the review and oversight of security matters. The Mint[41] and GA had established dedicated security committees, while at the ACC, security issues were canvassed as part of the agenda of a broader-focused operational management committee—known as the Organisation Health Committee (OHC).

2.10 The relevant governance committees at the ACC and GA both have wide-representation from across the agencies' operational areas and meet on a monthly and quarterly basis respectively. This broad representation helps facilitate informed discussions and decision-making. It also contributes to enhanced information sharing and increased awareness of security activities across the agencies. While the Mint's security committee has limited membership, the security team also regularly attend meetings of a number of the agency's other key governance forums, such as the Senior Management Forum and the Audit Committee.

[40] AGD, *Protective security governance guidelines: ASA and ITSA functions and competencies*, September 2011, pp. 4–5.

[41] Owing to the level of ongoing communication that occurs between members of the Mint's security committee, formal meetings are only convened on an as-needs basis. At the time of the audit, the committee had not formally met in the last two years.

Monitoring and reporting

2.11 Agencies should have structured processes in place for regularly assessing the continued effectiveness, appropriateness and relevance of the agency's security policies, plans and activities. Periodically, the agency's senior leaders and key governance forums should be provided with details of the status of protective security arrangements, including details of the results of the assessments of security risks and associated controls.[42] In 2013, agencies were required to undertake a self-assessment of, and report on, their compliance with the PSPF's 33 mandatory requirements.[43]

Defining a security assurance strategy

2.12 An assurance strategy can help guide the approaches required to be taken to monitor and report on the ongoing effectiveness of an agency's security policies and control measures relative to the evolving risk environment.

2.13 The Mint was the only agency that had defined a security assurance strategy. The Mint's assurance requirements were documented in its *Security Governance* procedures, which sets out the need for regular monitoring and review of its security management activities. Among other things, the document: outlines the responsibilities of the relevant security personnel; documents the Mint's security compliance assessment process (including for the requirements of the PSPF); and includes a template for assessing (and reporting) compliance.

2.14 Agencies should develop a security assurance strategy to assist with monitoring both the performance and conformance aspects of their protective security arrangements.

[42] As discussed in Chapter 3, regular monitoring and analysis is a key element of security risk management.

[43] Agencies were required to report their compliance with the PSPF's mandatory requirements to their portfolio Minister, the AGD and the Auditor-General.

Recommendation No.1

2.15 To strengthen security assurance and monitoring arrangements, the ANAO recommends that agencies implement a security assurance strategy that outlines their approach to monitoring:

- compliance with the PSPF and the agency's security policies; and
- the ongoing effectiveness of the agency's security policies and control measures.

Agency responses to Recommendation No.1

ACC's response

2.16 *Agree.*

AGD's response

2.17 *AGD supports this recommendation.*

GA's response

2.18 *Accepted.*

Mint's response

2.19 *Acknowledge and agree.*

Managing security incidents

2.20 Agencies are required by the PSPF to identify, manage and respond to security incidents. Monitoring security incidents can provide agencies with insights into the effectiveness of their physical security activities—including those controls implemented to mitigate the risks and threats faced by the agency.

2.21 Each of the audited agencies had security incident management processes and procedures, including guidance to staff on how to record, review, escalate, resolve and report the incidents. The agencies also had appropriate tools for managing security incidents, such as automated registers to capture (and enable reporting of) details of security incidents. Each of the agencies used qualified security investigators to examine security incidents, as deemed appropriate.

Reporting

Internal

2.22 Timely and well-designed management reports are important to help ensure that key stakeholders are informed about security matters, and better placed to make decisions.

2.23 Each of the agencies had processes in place to disseminate key security information to senior leaders. For instance the:

- ACC prepares security performance reports on a monthly basis for its senior management team, including details of progress against the 'business improvements' identified in the Commission's security plan and a summary of relevant information from its security incident management tool; and
- Mint provides quarterly status reports to its Audit Committee. These reports outline any key changes to the Mint's security arrangements, for instance changes related to compliance with the PSPF requirements or arising from security incidents.

Attorney-General's Department

2.24 As mentioned in Chapter 1, in 2013, agencies were required to undertake a self-assessment of, and to report on, their compliance with the PSPF's 33 mandatory requirements.

2.25 Each of the audited agencies submitted their self-assessment report against the PSPF mandatory requirements in September 2013 as required. Table 2.2 summarises the details reported by the agencies in their submissions, for the 16 mandatory requirements in scope for this audit.

Table 2.2: Self-assessment compliance reported by the audited agencies

Agency	Compliant	Partially compliant	Non-compliant	Total
ACC	16	0	0	16
GA	12	3	1	16
Mint	16	0	0	16

Source: The agencies' submissions.

2.26 The ANAO's assessment of the agencies' compliance with the PSPF mandatory requirements relevant to this audit was broadly consistent with the agencies' self-assessments. The ANAO downgraded the agencies' self-assessment ratings in 14 instances. Specifically, in:

- one case at GA, the ANAO considered the rating of 'compliant' to be 'non-compliant';
- 12 cases (nine at the ACC and three at GA) the ANAO considered the ratings of 'compliant' to be 'partially compliant'; and
- one case at GA, the ANAO considered the rating of 'partially compliant' to be 'non-compliant'.

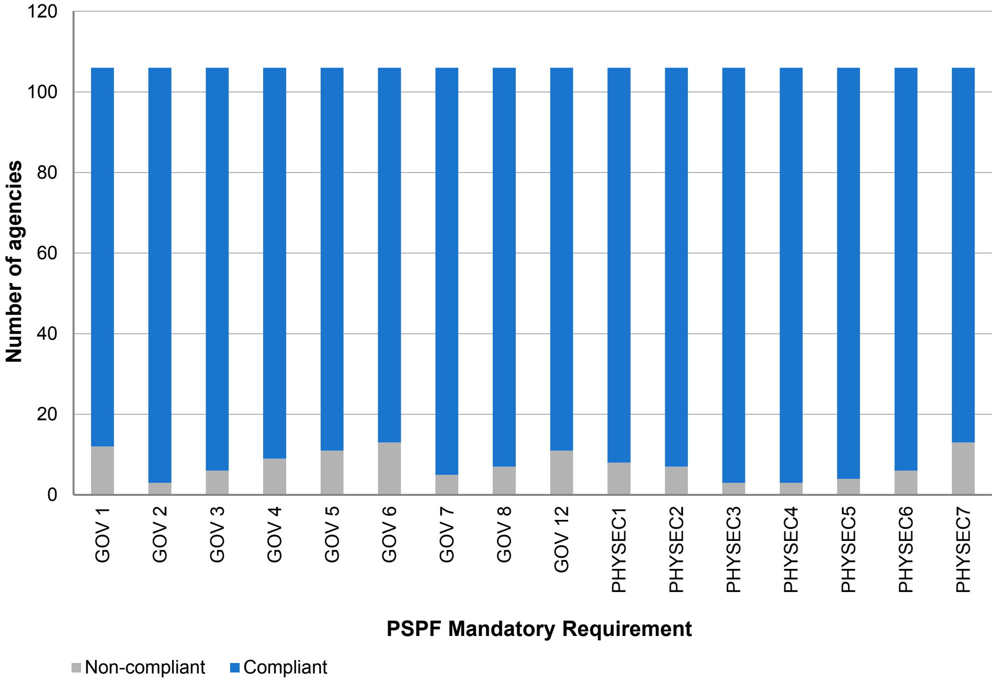
2.27 Further, the ANAO upgraded a self-assessment rating at GA—from 'partially compliant' to 'compliant'—to reflect improvements made by GA since September 2013.

2.28 Figure 2.1 provides an overview of the self-assessed compliance or non-compliance levels reported to AGD[44], for each of the 16 governance and physical security mandatory requirements examined in this audit.[45] As shown in Figure 2.1, overall, the average reported level of compliance with the mandatory requirements examined in this audit was around 90 per cent.

[44] AGD received responses from 110 entities, including 101 FMA Act agencies and nine CAC Act bodies. Four of the 110 entities provided classified responses, which are not included in the analysis shown in this report.

[45] Appendix 4 contains further analysis of the reported level of agencies' self-assessed compliance or non-compliance with the 16 mandatory requirements examined in this audit. Figure A.1 shows the level of compliance and non-compliance by agency size; and Figure A.2 shows the level of compliance and non-compliance by agency group.

Figure 2.1: Reported compliance and non-compliance by mandatory requirement



Source: ANAO, based on data from AGD.

2.29 In their reports to the AGD, the ACC and GA adopted a three-level rating system—'compliant', 'partially compliant' or 'non-compliant'. This approach was inconsistent with the reporting guidance contained in the PSPF.[46] Specifically, the guidance proposes that the status of each mandatory requirement be reported as 'fully compliant', 'non-compliant' or 'not applicable'. In cases of non-compliance, the guidance suggests that further details—such as mitigation measures and residual risks—should also be supplied.

2.30 The ANAO observed that the binary (fully compliant or non-compliant) approach proposed by the AGD for reporting agencies' self-assessments does not adequately:

[46] AGD, *Protective Security Governance Guidelines: Compliance Reporting*, March 2012, pp. 10–11.

- reflect circumstances where agencies may have met most aspects of a particular requirement, but have outstanding actions (at the time of preparing their report) to demonstrate full compliance; or
- capture agencies' progress as they work towards an improved level of compliance.

2.31 In the course of this audit, the AGD advised that it plans to develop additional guidance material for agencies' self-assessment and reporting, and is also investigating the potential for using a 'maturity level model' for PSPF reporting.

Information sharing and collaboration

2.32 Sharing of information between, and collaboration with, pertinent internal stakeholders can provide useful insights for managing protective security. The PSPF reinforces the importance of having such communication channels through its mandatory requirements, particularly PHYSEC 3.[47] The PSPF also encourages agencies to consult with other government agencies about security matters, including seeking advice for their security risk assessments. External communication and consultation may assist agencies to identify and consider a broader range of security issues and risks; and drawing on the insights and experiences of broadly comparable organisations can offer particular benefit.

Internal communication

2.33 The audited agencies have developed policies and procedures to support internal communication about physical security matters. Most notably, this included:

- requirements for security teams—at all agencies—to be involved in activities with physical security implications, such as during the design or modification of facilities;
- the Mint's security team being involved with a number of the agency's key governance forums; and

[47] PHYSEC 3 requires agencies to ensure that they integrate consideration of protective security matters into the process of planning, selecting, designing and modifying their facilities.

- the ACC's and GA's main security governance committees comprising representatives from across the agencies.

2.34 However, only the Mint was able to demonstrate that it had effective communication arrangements in practice. Arrangements in GA and the ACC were mostly informal and the agencies were unable to demonstrate that their internal requirements were consistently applied.

Consulting with other Australian Government agencies

2.35 The ACC and the Mint advised that their ASAs regularly engaged with ASAs in other agencies. The agencies advised that consultations tended to relate to general knowledge sharing or discussions on broader security-related matters; and did not generally extend to the identification of agency-specific security risks or security management activities.

Assessment of compliance with mandatory requirements and implementation of previous ANAO recommendations

2.36 Table 2.3 shows the results of the ANAO's assessment against the mandatory requirements relevant to the matters considered in this chapter.

Table 2.3: Assessment against mandatory requirements

Mandatory requirement	Result	
GOV 2—roles and responsibilities	All of the audited agencies were assessed as compliant with this requirement.	
GOV 3—ASA and ITSA knowledge	All of the audited agencies were assessed as compliant with this requirement.	
GOV 7—PSPF self-assessment and reporting	All of the audited agencies were assessed as compliant with this requirement.	
GOV 8—security investigators	All of the audited agencies were assessed as compliant with this requirement.	
GOV 12—contractors' compliance	ACC	Partially compliant—the standard contractual clauses can be improved to provide more detailed guidance to contracted service providers about the ACC's physical security requirements.
	GA	Compliant.
	Mint	Compliant.
PHYSEC 2—management of security incidents	All of the audited agencies were assessed as compliant with this requirement.	
PHYSEC 3—integration of physical security into facilities management	ACC	Partially compliant—the ACC's documented policies for engaging the ASA and ITSA in the design and modification of facilities in a timely way are not being consistently applied.
	GA	Compliant.
	Mint	Compliant.
PHYSEC 4—physical security and Work Health and Safety(WHS) obligations	ACC	Partially compliant—while the ACC has established a committee to oversee WHS in the agency, there is only limited interaction between the security team and business areas about WHS issues.
	GA	Non-compliant—GA was unable to demonstrate a consistent level of consideration of the risks associated with WHS obligations.
	Mint	Compliant.

Source: ANAO.

2.37 Table 2.4 shows the results of the ANAO's assessment against the previous ANAO recommendation relevant to the matters considered in this chapter.

Table 2.4: Implementation of previous ANAO recommendation

Previous ANAO recommendation	Result
Audit Report No.23, 2002–03 Recommendation 6—improving recording and reporting of security incidents	All of the audited agencies were assessed as having implemented the recommendation.

Source: ANAO.

Conclusion

2.38 Sound arrangements for the delivery and oversight of physical security activities were in place at each of the selected agencies. Specifically, each of the agencies had clearly identified the key security roles and responsibilities required by the PSPF, and the personnel appointed to these roles had an appropriate level of knowledge, skills and experience, enabling them to fulfil their duties. Importantly, all agencies had established forums to oversee and support the management of physical security—the Mint and GA had established dedicated security committees, while the ACC had a broader-focused operational management committee where security related matters could be raised.

2.39 At an operational level, all the agencies had processes and procedures to identify and manage day-to-day physical security incidents. However, the Mint was the only agency that had developed a security assurance strategy to outline its approach to the oversight and monitoring of security requirements; an arrangement that all agencies should adopt. See recommendation no. 1 at paragraph 2.15.

2.40 Each of the audited agencies submitted their first self-assessment compliance report against the PSPF's mandatory requirements to the AGD in September 2013, as required. In doing so, the ACC and GA adopted a three-level rating system—'compliant', 'partially compliant' or 'non-compliant'. However, this approach was inconsistent with the reporting guidance in the PSPF. Specifically, the guidance proposed that the status of each mandatory requirement be reported as 'fully compliant', 'non-compliant' or 'not applicable'. In cases of non-compliance, the guidance suggested that further details—such as mitigation measures and residual risks—should also be supplied.

2.41 The ANAO observed that the binary (fully compliant or non-compliant) approach proposed by the AGD does not adequately reflect circumstances where agencies may have met most aspects of a particular requirement, but have outstanding actions (at the time of preparing their report) to demonstrate full compliance. Further, it does not capture agencies' progress as they work towards an improved level of compliance. In the course of this audit, AGD advised that it plans to develop additional guidance material for agencies' self-assessment and reporting, and are also investigating the potential for a 'maturity level model' for PSPF reporting.

2.42 The Mint had structured arrangements in place to support ongoing communication and collaboration between the security team and key internal stakeholders—including 'health and safety' staff—and other government agencies. Equivalent arrangements in the ACC and GA were mostly informal and the agencies were unable to demonstrate that these arrangements were consistently applied.

3. Security Risk Management

This chapter discusses the results of the ANAO's examination of the selected agencies' security risk management arrangements.

Introduction

3.1 Australian Government agencies face a range of common security risks. These include risks that may affect: the integrity of their information and physical resources; the Commonwealth's reputation; performance against their objectives; and the safety of their staff or the public that deal with the agency.[48] Establishing and maintaining structured processes, which are designed in light of the agency's operating context and environment, is an important element in managing security risks.

3.2 The PSPF highlights the benefits of adopting the following security risk management principles as part of a common approach to managing protective security:

- security risk management should be part of each staff members' and contracted service providers' day-to-day responsibilities;
- the process for managing security risk should be logical and systematic, and be integrated into agencies' enterprise-wide monitoring and management processes; and
- the security threat environment should be regularly monitored and adjustments made, as necessary, to maintain an appropriate balance between an acceptable level of security risks and agencies' operational needs.

3.3 In evaluating the selected agencies' security risk management activities, the ANAO considered:

- approach and methodology—a security risk management approach has been defined, covering risk identification, assessment and monitoring; and
- links with policies and plans— agency security documentation reflects the results of security risk management activities.

[48] ANAO, Audit Report No.44 2008–09, *Security Risk Management*, p. 28.

Approach and methodology

3.4 The PSPF requires agencies to adopt a risk-based approach to the development and management of their protective security measures and arrangements.[49] Specifically, the PSPF states that an agency's approach to security risk management must be in accordance with the *AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines* and *HB 167:2006 Security Risk Management.*[50]

3.5 Table 3.1 shows the broad elements of a security risk management process.

Table 3.1: Broad elements of security risk management

Element	Description
Establish the context	Develop the scope of the risk management exercise and the criteria to be used to analyse and evaluate security risks. Consider the level of risk that the agency is prepared to accept and determine the level of resources available.
Identify the risks	Identify the security risks to the agency by assessing the nature and source of the harm that could occur to its key functions and official resources—such as its people, information and assets.
Analyse the risks	Analyse each identified security risk to determine how significant (in terms of its consequence and likelihood) the potential risk is to the agency. Develop a rating for each risk.
Evaluate the risks	After taking into account the strength of the controls and treatments already in place, consider whether there are any residual security risks that are unacceptable.
Treat the risks	Develop appropriate options or strategies to reduce or mitigate against the residual security risks that are deemed to be unacceptable. Document details of these strategies, including the internal responsibilities for them, in the security plan.
Monitor the arrangements	Regularly monitor the implementation of any additional controls or strategies and regularly review the ongoing effectiveness of the existing security controls. Also regularly monitor the identified risks and their analysis and evaluation.

Source: ANAO, based on *HB 167:2006 Security Risk Management.*

[49] AGD, *Securing Government Business: Protective Security Guidance for Executives*, May 2013, p. 3. Available from: <http://www.protectivesecurity.gov.au/pspf/Documents/Securing%20Government%20Business%20-%20Protective%20Security%20Guidance%20for%20Executives.pdf>. [Date accessed: 3 May 2014].

[50] PSPF mandatory requirement GOV 6.

Framework and guidance

3.6 All of the audited agencies had established structured enterprise-wide risk management policies and methodologies. The risk management methodology adopted by each agency, as outlined in their policy and procedural documents, was consistent with the requirements of *AS/NZS ISO 31000:2009*. However, the Mint was the only agency that had developed a security-specific risk management process. In particular, the Mint's security risk management policy and procedural document contains:

- a description of the Mint's approach to security risk management;
- reference to the Mint's corporate risk management policy—which contains further guidance on the conduct of risk assessments;
- guidance on performing security threat assessments;
- guidance on business impact levels;
- guidance on implementing control measures to mitigate security risks; and
- information on the application of a multi-layered system of control measures for managing security risks—known as 'security-in-depth'.

3.7 Neither the ACC nor GA had any targeted policy or procedural documentation to inform staff about arrangements for managing security risks or the conduct of security risk assessments. The ACC's corporate risk policy manual does, however, illustrate the agency's approach to security risk management—employing a diagram extracted from *HB 167:2006.*

3.8 This lack of procedural guidance on the approach to security risk management is considered to contribute, at least in part, to the ANAO's assessment that the security risk assessments conducted by the ACC and GA did not fully align with the requirements of the PSPF—this is shown in Table 3.2.

Integrating security risk management into corporate risk management activities

3.9 The PSPF states that an agency's security risk management activities should be integrated into, or otherwise aligned with, other corporate risk activities in the agency. Specifically, in a well-designed and integrated approach, agencies are likely to be better placed to identify and deal with security threats and issues. Such an approach also promotes better awareness of security issues across the agency. The absence of such an approach may mean that security risk management activities are:

- treated only as an enabler or support or peripheral function;
- not afforded sufficient priority or resources; or
- inconsistent with the agency's broader risk priorities and strategies.[51]

3.10 The Mint has a number of strategies to help align its security risk management activities and other corporate risk activities. These include:

- reviewing the Mint's operational risk registers on a quarterly basis, including the *Protective Security Risk Register*, and determining if changes are required to the agency's *Strategic Risk Profile*[52]*;* and
- regularly preparing reports on risk management activities for the Mint's Chief Executive Officer.

3.11 At the time of the audit, both the ACC and GA were in the process of implementing arrangements to enhance links between security risk activities and other corporate risk activities. For instance, GA advised that it is updating its corporate risk management policy to provide 'greater consistency and transparency' between the agency's various risk management activities. Specifically, it advised that security will be recognised as a category of the risks faced by GA. Further, both GA and the ACC advised the ANAO of increased levels of collaboration between their security teams and other corporate risk management functions, including: through greater sharing of information; and increased representation from both teams at relevant governance meetings or discussions.

The conduct of security risk assessments

3.12 The PSPF requires agencies to identify security-related risks to their people, information and assets, and to continually assess these risks. Within the broad steps outlined in Table 3.1, some of the key aspects in the conduct of a security risk assessment prescribed in the PSPF are:

[51] ANAO, op. cit., p. 47.

[52] The *Strategic Risk Profile* contains details of those risks, including security risks that are assessed as impacting on the Mint achieving its strategic objectives. The profile is regularly reviewed by several of the Mint's key governance forums, including the Audit Committee.

- identify those assets that are critical to the ongoing operations of the agency or to the national interest;
- assess the threats and risks against those critical assets;
- identify and assess risks relating to harm to the public;
- assess the business impact levels for the critical assets;
- identify risks and threats associated with heightened threat levels;
- identify and assess site-specific risks; and
- ensure WHS obligations are considered.

3.13 All agencies had undertaken recent security risk assessments. Each of the assessments examined, captured and assessed key security risks, and outlined recommendations or risk mitigation actions to be undertaken. However, as shown in Table 3.2, the Mint was the only agency that adopted practices that aligned with each of the key aspects prescribed in the PSPF.

Table 3.2: Agencies' security risk assessment practices against key aspects prescribed in the PSPF

PSPF prescribed step	ACC	GA	Mint
Identification of critical assets	✓[A]	✓	✓
Assess the risks and threats to the critical assets	✓[B]	✓	✓
Identify and assess risks relating to harm to the public			✓
Assess the business impact levels			✓
Assess heightened threat levels	✓[C]		✓
Assess site-specific risks	✓[D]	✓	✓
Integrate WHS obligations	✓		✓

Source: ANAO.

Notes:

A: The ANAO observed that the ACC has identified critical assets as part of its new approach to performing site security risk assessments—which was introduced during the audit.

B: The ACC advised the ANAO that it will be assessing risks to critical assets as part of a new approach to performing site security risk assessments.

C: The ANAO suggested that the ACC's policy could be enhanced by including details of the measures or strategies in place to reduce the impact of operating at heightened threat levels.

D: The ACC has drafted a site security plan for its ACT office, but this had not been approved at the time of the audit. The ACC advised that the remaining site security plans will then be developed using the approved format. This is discussed further at paragraph 3.16.

3.14 Agencies had procedures for responding to certain emergencies, such as receipt of a suspicious package or responding to a bomb threat. However, only the Mint and ACC had developed policies specifically outlining operational requirements in situations of heightened threat or security levels. Notably, the Mint has established separate governance arrangements to oversee planning for, and the agency's response to, heightened threat levels—the Mint's ASA is a member of these forums.

3.15 While agencies' security risk assessments considered risks to staff, the assessments prepared by the ACC and GA had not explicitly identified risks relating to general members of the public. This was a significant omission at GA, which has a large number of visitors to its premises.[53] While the ACC does not typically have members of the public visit its premises, there are some parts of its operations which involve interactions with the public.

3.16 The PSPF also states that an agency should identify and assess security risks that are unique to each of its operational sites. GA and the Mint had performed site security risk assessments, although GA's assessment was out of date. A broad-based security risk assessment completed by the ACC in 2012 identified the need to undertake site-specific security risk assessments, and to prepare site-specific security plans.[54] At the time of the audit, the ACC had performed a security risk assessment, and drafted a security plan, for its ACT office. The ACC informed the ANAO that if endorsed by senior management, the ACT security plan would be used as a template for its other offices.

Monitoring security risks

3.17 Only the Mint was able to demonstrate that it had structured arrangements in place for monitoring security risks—including the continued effectiveness of security risk treatments or controls— that were consistently applied. Among the practices observed at the Mint, was that the ASA regularly monitors the appropriateness of the risks and treatments contained in the Mint's *Protective Security Risk Register.* The Mint also advised that additional risks will be added to the register, as necessary. For instance, an emerging risk can be identified as a result of information collected during security incident reporting.

[53] 16 000 members of the public visit GA annually, including school groups.

[54] The security risk assessment noted that this was important in order for the ACC to better manage the security risks unique to each of its locations.

3.18 Arrangements in place for monitoring security risks at GA and the ACC tended to be less structured and ad hoc. For instance, the ACC advised that while it does not have an explicitly defined process, it considers that monitoring of security risks and controls occurs as part of the agency's day-to-day 'business as usual' activities.

Links with policies and plans

3.19 Well-designed security policies and plans are key sources of information and instruction for staff fulfilling security-related responsibilities. In particular, security policies and plans will help promote consistent understanding of security standards and expected behaviours across the agency.[55]

3.20 The PSPF outlines[56] that an agency's:

- protective security policy should articulate the outcomes to be achieved by protective security; and
- protective security plan should set out the strategies and actions necessary to achieve the outcomes from the protective security policy.

3.21 The PSPF also states that an agency's protective security policies and plans should be informed by the agency's security risk assessments. Specifically, this means that the agency's protective security policies and plans need to be aligned to the outcomes of their security risk assessment.

3.22 The Mint was the only agency able to demonstrate a clear linkage between the outcomes of its security risk assessment and its security policies, plans and procedures. For instance, the Mint's protective security plan identifies the control measures required to be implemented to reduce those risks identified as being an unacceptably-high residual risk. The Mint's security plan also includes details of the: associated costs; staff member responsible for implementing the control; target date for implementation; and the implementation status of the additional control.

[55] ANAO, op. cit., p. 34.

[56] Attorney-General's Department, *Protective security better practice guide – Developing agency protective security policies, plans and procedures*, March 2012, available at <http://www.protectivesecurity.gov.au/governance/developing-a-security-culture/Pages/Better-practice-guide-on-developing-a-security-culture.aspx>. [Date accessed: 23 August 2013].

3.23 At the time of the audit, both the ACC and GA advised that they were in the process of updating their key security documents to better reflect the results of their most-recent security risk assessments—finalised in January 2013 and June 2012 respectively. In addition, the ACC was in the process of conducting a series of site-specific security risk assessments, and advised that its security policies and plans would be further updated, as necessary.

3.24 Agencies should align security policies and plans with the outcomes of their security risk assessment activity.

Recommendation No.2

3.25 To assist agencies to adopt and maintain an effective approach to the management of physical security risks, the ANAO recommends that agencies, in the context of their discrete operating circumstances:

- integrate security risk management activities with other organisational risk activities;
- tailor procedures for the conduct of security risk assessments that align to the requirements of the PSPF; and
- update security policies and plans to reflect the outcomes of security risk assessments.

Agency responses to Recommendation No.2

ACC's response

3.26 *Agree, noting that security policies and plans in the ACC do reflect the outcome of security risk assessments and are updated when required.*

AGD's response

3.27 *AGD supports this recommendation.*

GA's response

3.28 *Accepted. Geoscience Australian is currently reviewing its risk management framework to ensure that the framework provides a holistic approach to risk across the agency, including security risks. The outcome of risk assessments will be used to update other relevant agency documents, including security policies and plans.*

Mint's response

3.29 *Acknowledge and agree.*

Assessment of compliance with mandatory requirements and implementation of previous ANAO recommendations

3.30 Table 3.3 shows the results of the ANAO's assessment against the mandatory requirements relevant to the matters considered in this chapter.

Table 3.3: Assessment against mandatory requirements

Mandatory requirement	Agency	Result
GOV 4—security plans	ACC	Partially compliant—the ACC's security plan does not address some of the matters outlined in the PSPF and does not align with the outcomes of its security risk assessment. At the time of the audit, the ACC was in the process of preparing a more-detailed security plan for its ACT office. The ACC advised that if approved, the ACT plan will be used as a template for the development of further site specific security plans.
	GA	Partially compliant—GA's security plan is outdated and does not align with the most recent security risk assessment. GA advised the ANAO that a process to review and update the plan is underway.
	Mint	Compliant.
GOV 5—security policies and procedures	ACC	Partially compliant—the ACC's security policy and procedural manual does not align with the outcomes of its security risk assessment. The ACC informed the ANAO that review processes are underway to update the document.
	GA	Partially compliant—GA's security policy has been recently updated to reflect its security risk assessment. At the time of the audit, GA was revising other security documentation and procedures to ensure they align with the outcomes of its most recent security risk assessment.
	Mint	Compliant.
GOV 6—risk management approach	ACC	Partially compliant—the security risk assessment approach undertaken by ACC is not consistent with the guidance provided by the PSPF. During the audit, the ACC advised the ANAO that changes are in train to update and improve its approach to security risk management.
	GA	Partially compliant—some improvements are necessary to ensure that the GA's approach to security risk management aligns with the requirements of the PSPF.
	Mint	Compliant.
PHYSEC 1—physical security policies and plans	ACC	Partially compliant—as per GOV 4 and GOV 5.
	GA	Partially compliant—as per GOV 4 and GOV 5.
	Mint	Compliant.

Mandatory requirement	Agency	Result
PHYSEC 5—duty of care for the safety of the public	ACC	Partially compliant—the ACC has processes for promoting safety to visitors to the agency. However, the safety of the public has not been explicitly considered as part of recent security risk assessments.
	GA	Non-compliant—GA has not captured risks relating to public safety in its security risk assessments.
	Mint	Compliant.
PHYSEC 7—heightened threat levels	ACC	Partially compliant—the ACC's security documents contain some details relating to heightened threat levels. However, the ACC has not clearly articulated preventive strategies relating to operating at heightened threat levels.
	GA	Non-compliant—GA has not formally considered heightened threat levels.
	Mint	Compliant.

Source: ANAO.

3.31 Table 3.4 shows the results of the ANAO's assessment against the previous ANAO recommendations relevant to the matters considered in this chapter.

Table 3.4: Implementation of previous ANAO recommendations

Previous ANAO recommendation	Result	
Audit Report No.23, 2002–03 Recommendation 1—conduct comprehensive security risk assessments every three years	ACC	Implemented.
	GA	Not implemented—GA has not undertaken comprehensive security risk assessments at least every three years.
	Mint	Implemented.
Audit Report No.23, 2002–03 Recommendation 2—document decision-making processes relating to security treatments	ACC	Implemented.
	GA	Partially implemented—a majority of GA's security documents are outdated.
	Mint	Implemented.
Audit Report No.23, 2002–03 Recommendation 3 (part 1)—develop and document security plans and procedures	ACC	Partially implemented—the ACC has not defined a structured approach to the management of security documentation.
	GA	Partially implemented—GA is in the process of updating its key security documents.
	Mint	Implemented.
Audit Report No.23, 2002–03 Recommendation 4—risk assessments should address staff safety	ACC	Implemented.
	GA	Partially implemented—although GA's security risk assessment identified its staff as a 'critical asset', the assessment did not explicitly address the risks associated with staff safety.
	Mint	Implemented.
Audit Report No.23, 2002–03 Recommendation 5—security risk assessments address requirements relating to security classified information	ACC	Implemented.
	GA	Partially implemented—GA is currently in the process of revising and updating key security documents.
	Mint	Implemented.

Source: ANAO.

Conclusion

3.32 While each of the agencies had formal enterprise-wide risk management policies and procedures, only the Mint had clearly defined its approach to, and methodology for, the management of security risks.

3.33 Each agency had recently conducted an assessment of security risks and associated treatment options. However, the Mint was the only agency that had consistently implemented the full range of security-specific risk management practices required by the PSPF, being the: identification of critical assets; assessment of business impact levels; assessment of risks to the public; identification of site-specific risks and development of associated plans; and assessment for heightened threat levels. The ACC and GA had established some of these measures but not all, or had not applied them on a consistent basis.

3.34 The Mint demonstrated that it had an integrated approach to aligning security risk management activities with other organisational risk activities, such as fraud control planning. An integrated approach facilitates internal understanding and assessment of the interdependencies between security risks and other risks.

3.35 The Mint was also able to demonstrate that its security policies and plans had been updated and aligned to the outcomes of its most recent security risk assessment. At the time of the audit, both the ACC and GA advised that they were in the process of doing so—having finalised their protective security risk assessments in January 2013 and June 2012 respectively.

4. Control Activities

This chapter discusses the results of the ANAO's examination of the selected agencies' security control activities.

Introduction

4.1 To effectively manage their physical security risks and threats, agencies will typically need to have a range of measures, processes or controls in place. To help staff better understand the nature and purpose of these controls, including responsibilities for their effective day-to-day operation, agencies should have:

- appropriately tailored procedural documentation that is aligned with their security policies and plans; and
- well-designed security awareness and training programs, including a range of mechanisms to promote security awareness.

4.2 In evaluating the selected agencies' control activities, the ANAO considered the following:

- management of security documentation—there is a structured approach to the development and maintenance of security documentation;
- security procedures in practice—key security procedures are operating as intended and support physical security management; and
- training and awareness—to promote security awareness within the organisation there is a defined approach to security training for staff and for contracted service providers.

Management of security documentation

4.3 A structured approach to the development and maintenance of key security documents—security policies, plans and associated procedural material—can assist agencies to build and maintain a stronger security culture. In particular, such an approach can help equip staff to better understand and meet their security-related responsibilities. A well-designed approach will support:

- consistency in the documents' management;
- clarity of intent and purpose for the documents;

- the identification of links or references between the documents;
- the setting of timeframes for reviewing the currency and continued appropriateness of the documents; and
- storage of the documents in a manner that is easy for staff to access.

4.4 GA and the Mint had both defined their approach to the development and maintenance of key security documents, and documented the hierarchy of—and linkages between—these key security documents. The Mint also published a visual representation of its security document management framework on its intranet, with hyperlinks to the various security documents.

4.5 The key security documents at the ACC and the Mint were found to be current—the conduct of the audit coincided with the ACC's annual review of its security documentation. At the time of the audit, GA advised that it was revising and updating its key security documents.

4.6 GA and the Mint publish key security documents on their intranets, which facilitates easy access to the documents. The ACC did not maintain security documents in a central location—some documents were stored on the ACC's intranet, while others were stored in its electronic document management system. Further, the ACC did not have a structured approach to maintaining document version control or ensuring only the current version was accessible—increasing the risk that staff may not be aware of the most recent procedures.

4.7 Table 4.1 illustrates the key security documents at each of the selected agencies.

Table 4.1: Key security documents observed at the audited agencies

Security document	ACC	GA	Mint
Agency security risk assessment	✓	✓	✓
Agency security policy	✓	✓	✓
Agency security plan	✓[A]	✓[B]	✓
Physical security policy	✓	✓	✓
Physical security procedures	✓[C]	✓[D]	✓

Source: ANAO.

Notes:

A: As discussed at paragraph 3.16, at the time of the audit the ACC had prepared (but had not endorsed) a security plan for its ACT office and advised that it plans to prepare further site-specific plans.

B: GA's security plan has not been updated since 2008. The GA security team has a *Work Plan* that documents the work required to comply with the requirements of the PSPF—this includes the review of GA's physical security plan and procedures. GA has advised that it anticipates its security plan and security manual will be updated and endorsed in early 2015.

C: ACC has a series of location-specific procedural documents. However it does not have mechanisms to ensure consistency in the form and content of such documents across the agency.

D: Contained in GA's *Security Manual*, which was last updated in 2008.

Security procedures in practice

4.8 The PSPF requires agencies to develop security procedures to manage their identified security risks.[57] The procedures should be aligned to the directions set out in their security policies and plans.

4.9 Examples of key physical security measures adopted by the audited agencies include:

- use of swipe access or electronic access control systems;
- wearing of identification passes;
- closed circuit television monitoring;
- use of security guards;
- visitor sign-in processes;
- secure containers and cabinets;

[57] PSPF mandatory requirement GOV 5.

- use of equipment endorsed by the Security Construction and Equipment Committee[58]; and
- security alarms, including remote monitoring.

4.10 The ANAO examined the operation of a number of the key processes and controls designed to protect information, staff and other resources at each of the selected agencies.[59] The ANAO's examination indicated that the key physical security procedures that had been implemented were generally operating as designed. Further, the controls and processes that were observed generally aligned with agency security policies, plans and procedural documentation. Overall, in each case, the ANAO considered the selected security controls and processes to be commensurate with the agencies' security risk profiles. In one agency, the controls examined incorporated key lessons learned from past experience.

Training and awareness

4.11 A program of security awareness and training—developed in the context of the agency's security threats and operating environment—can contribute to the effectiveness of an agency's protective security arrangements. Recognising this, the PSPF requires that agencies provide security awareness training to staff and contractors.[60] A well designed security awareness and training program should be designed to help foster a strong security culture within the agency by:

- promoting the importance of security;
- providing individuals with an understanding of their responsibilities under the agency's security policies and plans; and
- explaining the potential implications of breaches of security, as well as the associated reporting requirements.[61]

4.12 Effective implementation of the PSPF requirement relating to security awareness will include the provision of appropriate training for staff with specific security duties.

[58] The Security Construction and Equipment Committee is responsible for evaluating security equipment for use by Australian Government agencies, and preparing the *Security Equipment Evaluated Products List.*

[59] The ANAO examined the operation of these controls by performing walkthroughs of selected parts of the agencies' premises. During these walkthroughs, the selected security controls were discussed with key staff and the ANAO observed the selected procedures in operation.

[60] PSPF mandatory requirement GOV 1.

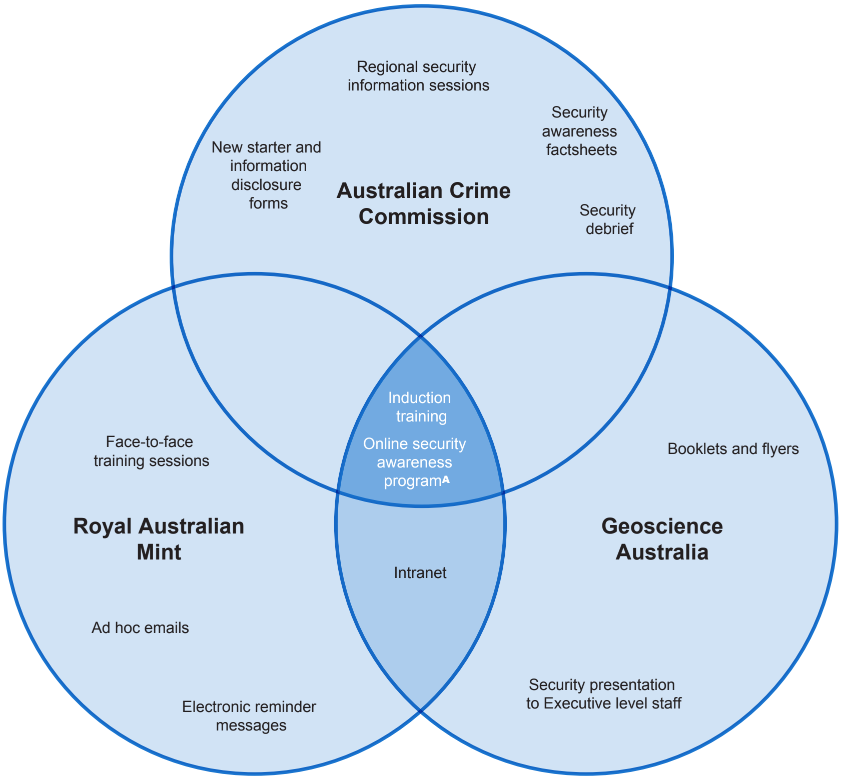
[61] ANAO, op. cit., p. 30.

Framework for promoting security awareness

4.13 Each of the agencies had put security training policies and strategies in place. These policies, which were readily available to staff, included a useful range of information such as: defining the agency's training delivery methods; and describing the coverage, frequency and target audience.

4.14 As illustrated in Figure 4.1, each agency had established a number of separate delivery channels to promote security awareness.

Figure 4.1: Channels for promoting security awareness


Regional security information sessions
New starter and information disclosure forms
Australian Crime Commission
Security awareness factsheets
Security debrief
Induction training
Online security awareness programA
Face-to-face training sessions
Royal Australian Mint
Booklets and flyers
Geoscience Australia
Intranet
Ad hoc emails
Electronic reminder messages
Security presentation to Executive level staff

Source: ANAO.

Note A: The Mint advised the ANAO that it is expecting to establish an online security awareness training program by the end of 2014.

4.15 Among the key initiatives observed during the audit were that:

- each of the agencies provided security information as part of their induction programs for new starters;
- the main security awareness and training program in each agency was required to be completed annually by all staff—in the ACC and GA this

was the on-line security awareness and training program, while at the Mint the main training vehicle was more-traditional face-to-face sessions; and

- the Mint and GA had consistent and structured processes for publishing security documents on their intranets, including security alerts and reminders.

4.16 In addition, the ACC advised the ANAO that the security team regularly analysed details of reported security incidents to identify common themes and as appropriate, develop security factsheets. These security factsheets were intended to inform and educate staff about contemporary, practical security issues facing the agency.

4.17 The ANAO examined the design and content of the key security awareness training delivery mechanism at each of the agencies. Overall, the training mechanisms examined were well-designed, providing an appropriate level of guidance and information about the agency's security arrangements, including details of security obligations and expectations. In particular, each of the packages included:

- an overview of protective security;
- details of the key security personnel and their responsibilities;
- an overview of physical, information and personnel security; and
- information on the agency's key security procedures, such as: information handling; security incident reporting; and security clearance requirements.

4.18 As shown in Table 4.2, there were generally high levels of completion-rates among staff for the agency's key security awareness training programs.

Table 4.2: Key security awareness training program completion statistics

	ACC	GA	Mint
Number of staff (at the time of the audit)	630	700	210
Completion rate	87%	96%	98%

Source: Training records at the selected agencies.

4.19 Each of the agencies advised that they had analysed the possible reasons for the relatively small proportions of staff that had not completed the security training, and had taken steps to address the issue. For instance, the ACC advised that its ASA makes contact with any staff who has been unsuccessful in passing the on-line training after three attempts. The ACC also advised that it had recently aligned completion of mandatory security training to the agency's performance management system.

Application of security requirements by contracted service providers

4.20 The PSPF makes it clear that agencies remain responsible for the management of security risks in cases where external service providers are engaged. Specifically, one of the PSPF's mandatory requirements is that agencies ensure contracted service providers comply with the standards and guidance contained in the PSPF.[62]

4.21 To assess if agencies were meeting this requirement, the ANAO examined whether the agencies had arrangements to provide contracted service providers with sufficient guidance to understand their security obligations and responsibilities.

4.22 All agencies required contracted service providers to complete security training once they were engaged. GA and the Mint required contractors to complete their respective security training packages. The ACC required contractors to attend security awareness information sessions or, in some cases, undertake more targeted security-related training. For example, the ACC's security guards routinely complete scenario-based training commensurate with their specific roles and responsibilities.

4.23 The selected agencies had also incorporated clauses in their contract templates to inform service providers about their security obligations and responsibilities. At GA and the Mint, these standard contract clauses covered a wide-range of operational security matters, including:

- handling of classified and confidential information;
- contractor security procedures;
- security incidents and reviews; and
- WHS obligations.

[62] PSPF mandatory requirement GOV 12.

4.24 At the ACC, the clauses contained in contract templates included higher-level statements, rather than prescriptive guidance. The ANAO suggested that the ACC examine opportunities to improve the level of guidance provided to contracted service providers. Providing further guidance would complement the ACC's targeted security awareness training activities and further contribute to contractors' understanding of their security obligations and responsibilities.

Training requirements for key security staff

4.25 The skills sets required of agency personnel responsible for managing physical security have changed over time. This change is largely due to the shift from the compliance-based approach to protective security inherent in the former Protective Security Manual (PSM), to the risk-based approach espoused in the PSPF. In particular, officers in key security roles, such as the ASE, the ASA and the ITSA, require new and updated skills to effectively identify and implement security policies and controls that are commensurate with their agency's threats and operating context.

4.26 Staff in key security roles had not received any targeted or advanced security-related training to help in the implementation of the PSPF. The Mint advised that it had assessed that its ASA did not require further training, as that official had undertaken a *Diploma in Risk Management*.

4.27 The Protective Security Training College, a part of AGD, provides protective security training for personnel from: Australian Government agencies; state and territory government agencies; and those private organisations responsible for the management of national critical infrastructure.[63] During the audit, the ANAO suggested to AGD that it review its approach to protective security training in light of the changing skills sets required for managing physical security. AGD informed the ANAO that it was reviewing the security training packages, including the levels of instruction and guidance on security risk management.

[63] National critical infrastructure provides services that are essential for everyday life, such as energy, food, water, transport, communications, health and banking and finance. A disruption to critical infrastructure assets could have a range of serious implications for business, governments and the community. See <http://www.ag.gov.au/NationalSecurity/InfrastructureResilience/Pages/default.aspx>. [Date accessed: 27 May 2014].

Assessment of compliance with mandatory requirements and implementation of previous ANAO recommendations

4.28 Table 4.3 shows the results of the ANAO's assessment against the mandatory requirements relevant to the matters considered in this chapter.

Table 4.3: Assessment against mandatory requirements

Mandatory requirement	Result
GOV 1—security awareness training	All of the audited agencies were assessed as compliant with this requirement.
PHYSEC 6—physical security measures relating to information and ICT equipment	All of the audited agencies were assessed as compliant with this requirement.

Source: ANAO.

4.29 Table 4.4 shows the results of the ANAO's assessment against the previous ANAO recommendations relevant to the matters considered in this chapter.

Table 4.4: Implementation of previous ANAO recommendations

Previous ANAO recommendation	Result
Audit Report No.25, 2009–10 Recommendations 2 and 3—security awareness and training	All of the audited agencies were assessed as having implemented the recommendation.
Audit Report No.23, 2002–03 Recommendation 3 (part 2)—security education and awareness programs for non-security staff	All of the audited agencies were assessed as having implemented the recommendation.

Source: ANAO.

Conclusion

4.30 The ANAO's examination of a selection of procedures and controls implemented to manage key physical security risks at each of the audited agencies, found that the controls were generally operating as intended. Importantly, the observed controls generally aligned with each agency's security policies, plans and procedural documentation.

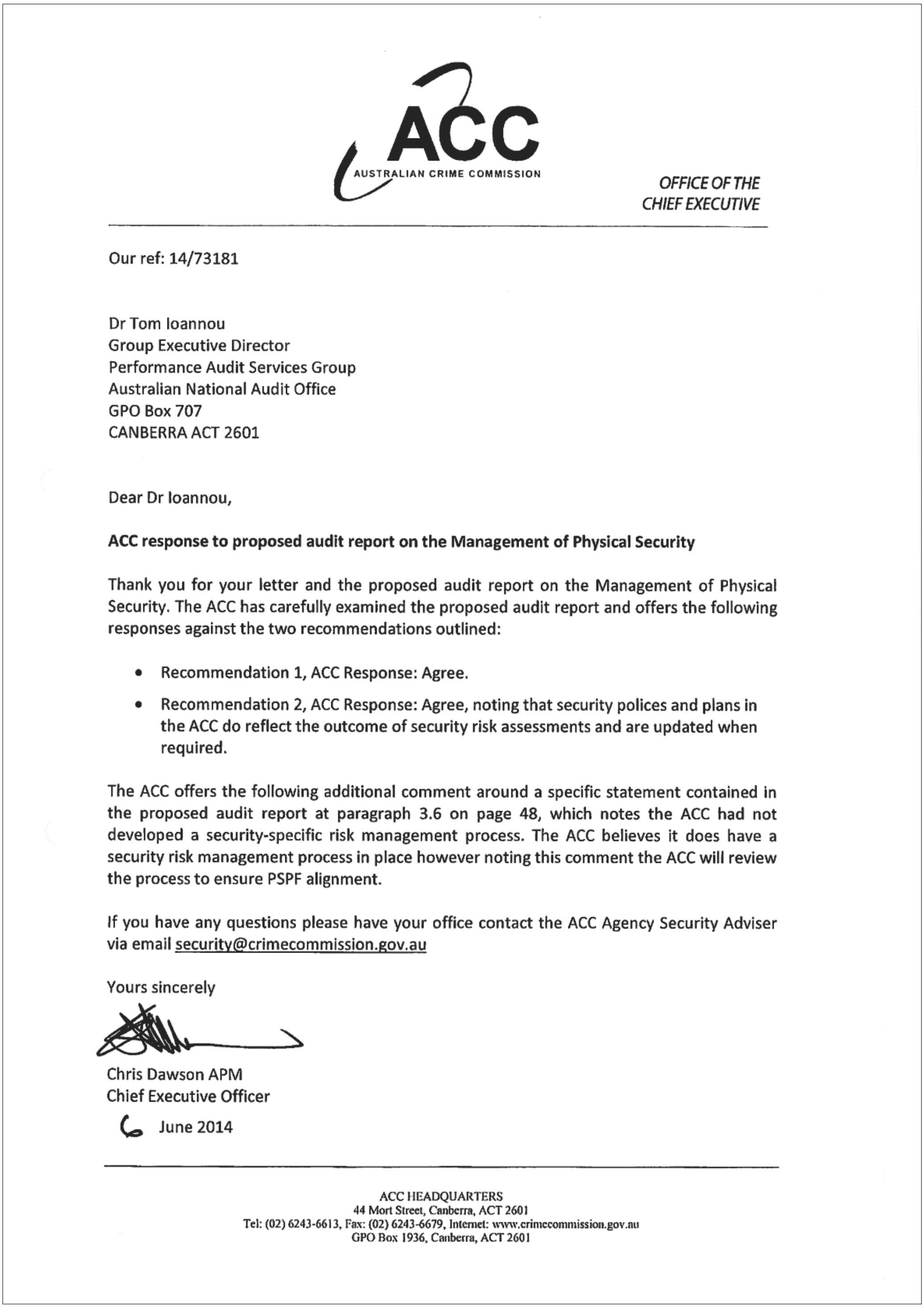
4.31 The agencies had established suitable security training and awareness programs using a range of communication methods and delivery channels. In each agency, the components of awareness and training programs that were examined during the audit were mandatory for all staff and incorporated content that was well-designed and informative. Notably, the content of each component of the security awareness training programs examined by the ANAO was consistent with the nature of each agency's security context. At GA and the Mint, service providers were also required to complete the security awareness training. Overall, completion rates of the security awareness training at the three agencies were generally high. The agencies advised that they had taken steps to address the issue of some staff not completing the training.

Ian McPhee
Auditor-General

Canberra ACT
24 June 2014

Appendices

Appendix 1: Agency responses



ACC
AUSTRALIAN CRIME COMMISSION

OFFICE OF THE
CHIEF EXECUTIVE

Our ref: 14/73181

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou,

ACC response to proposed audit report on the Management of Physical Security

Thank you for your letter and the proposed audit report on the Management of Physical Security. The ACC has carefully examined the proposed audit report and offers the following responses against the two recommendations outlined:

- Recommendation 1, ACC Response: Agree.
- Recommendation 2, ACC Response: Agree, noting that security polices and plans in the ACC do reflect the outcome of security risk assessments and are updated when required.

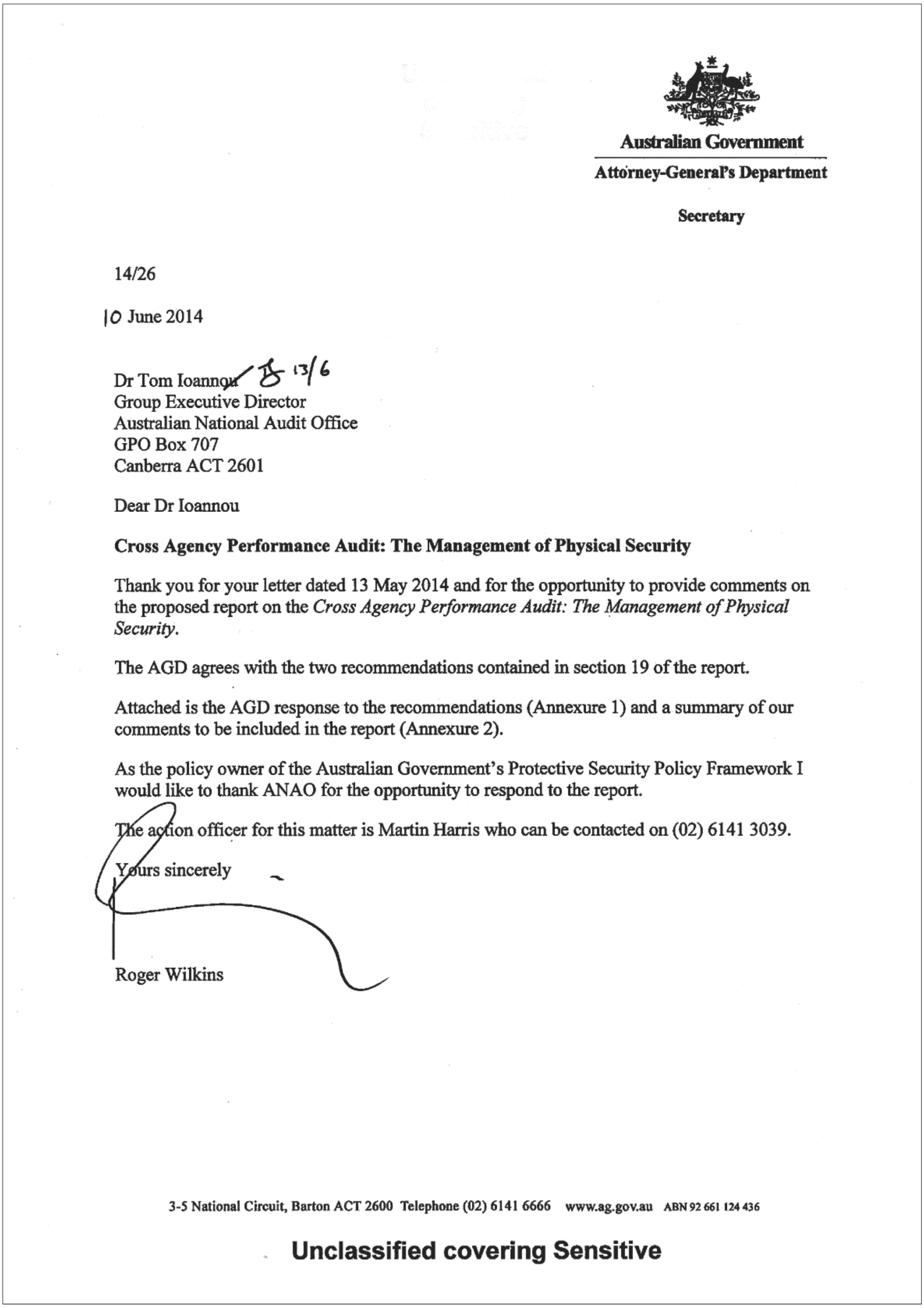
The ACC offers the following additional comment around a specific statement contained in the proposed audit report at paragraph 3.6 on page 48, which notes the ACC had not developed a security-specific risk management process. The ACC believes it does have a security risk management process in place however noting this comment the ACC will review the process to ensure PSPF alignment.

If you have any questions please have your office contact the ACC Agency Security Adviser via email security@crimecommission.gov.au

Yours sincerely

Chris Dawson APM
Chief Executive Officer
6 June 2014

ACC HEADQUARTERS
44 Mort Street, Canberra, ACT 2601
Tel: (02) 6243-6613, Fax: (02) 6243-6679, Internet: www.crimecommission.gov.au
GPO Box 1936, Canberra, ACT 2601



Australian Government

Attorney-General's Department

Secretary

14/26

10 June 2014

Dr Tom Ioannou 13/6
Group Executive Director
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Dr Ioannou

Cross Agency Performance Audit: The Management of Physical Security

Thank you for your letter dated 13 May 2014 and for the opportunity to provide comments on the proposed report on the *Cross Agency Performance Audit: The Management of Physical Security*.

The AGD agrees with the two recommendations contained in section 19 of the report.

Attached is the AGD response to the recommendations (Annexure 1) and a summary of our comments to be included in the report (Annexure 2).

As the policy owner of the Australian Government's Protective Security Policy Framework I would like to thank ANAO for the opportunity to respond to the report.

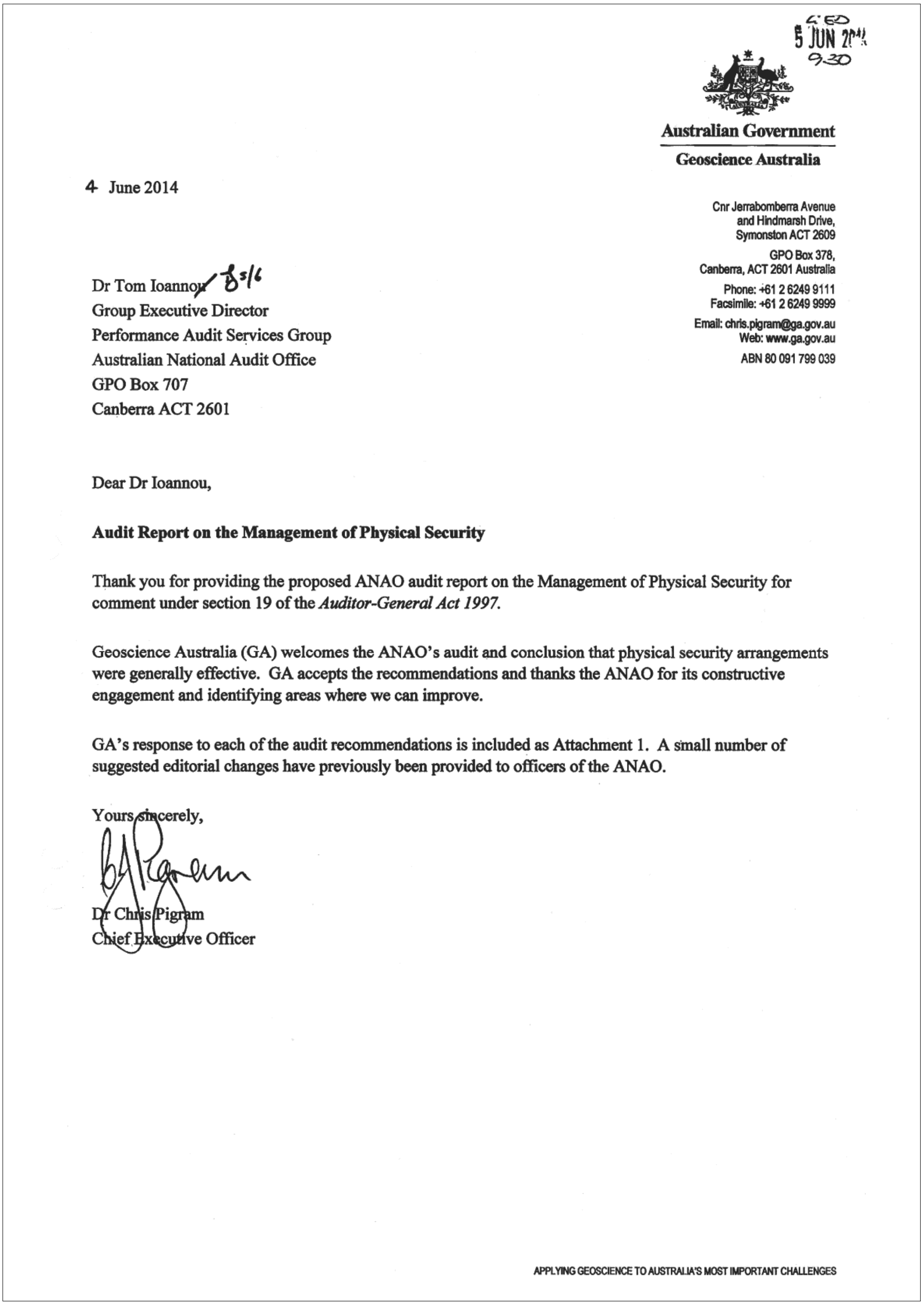
The action officer for this matter is Martin Harris who can be contacted on (02) 6141 3039.

Yours sincerely

Roger Wilkins

3-5 National Circuit, Barton ACT 2600 Telephone (02) 6141 6666 www.ag.gov.au ABN 92 661 124 436

Unclassified covering Sensitive



GED
5 JUN 2014
9.30

Australian Government

Geoscience Australia

4 June 2014

Cnr Jerrabomberra Avenue
and Hindmarsh Drive,
Symonston ACT 2609

GPO Box 378,
Canberra, ACT 2601 Australia

Phone: +61 2 6249 9111
Facsimile: +61 2 6249 9999

Email: chris.pigram@ga.gov.au
Web: www.ga.gov.au

ABN 80 091 799 039

Dr Tom Ioannou 5/6
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Dr Ioannou,

Audit Report on the Management of Physical Security

Thank you for providing the proposed ANAO audit report on the Management of Physical Security for comment under section 19 of the *Auditor-General Act 1997.*

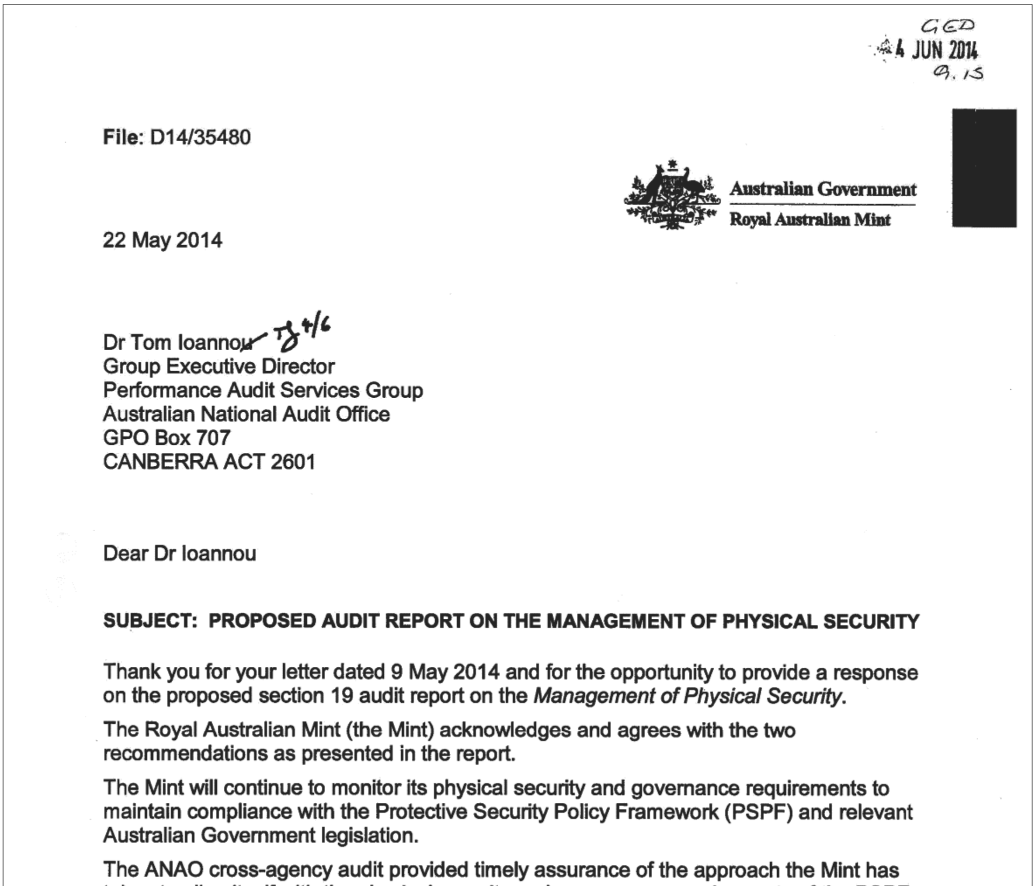
Geoscience Australia (GA) welcomes the ANAO's audit and conclusion that physical security arrangements were generally effective. GA accepts the recommendations and thanks the ANAO for its constructive engagement and identifying areas where we can improve.

GA's response to each of the audit recommendations is included as Attachment 1. A small number of suggested editorial changes have previously been provided to officers of the ANAO.

Yours sincerely,

Dr Chris Pigram
Chief Executive Officer

APPLYING GEOSCIENCE TO AUSTRALIA'S MOST IMPORTANT CHALLENGES



[redacted]

Australian Government
Royal Australian Mint

File: D14/35480

22 May 2014

Dr Tom Ioannou TJ 4/6
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou

SUBJECT: PROPOSED AUDIT REPORT ON THE MANAGEMENT OF PHYSICAL SECURITY

Thank you for your letter dated 9 May 2014 and for the opportunity to provide a response on the proposed section 19 audit report on the *Management of Physical Security.*

The Royal Australian Mint (the Mint) acknowledges and agrees with the two recommendations as presented in the report.

The Mint will continue to monitor its physical security and governance requirements to maintain compliance with the Protective Security Policy Framework (PSPF) and relevant Australian Government legislation.

The ANAO cross-agency audit provided timely assurance of the approach the Mint has taken to align itself with the physical security and governance requirements of the PSPF.

The Mint would also like to thank the ANAO for the professional conduct of the audit team including the collaborative working relationships formed with my staff during the course of the audit.

Yours sincerely

Ross MacDiarmid
Chief Executive Officer
Royal Australian Mint

DENISON STREET DEAKIN, CANBERRA ACT 2600 AUSTRALIA
NATIONAL 02 6202 6999 • INTERNATIONAL +61 2 6202 6999
FACSIMILE 02 6202 6935 • INTERNATIONAL +61 2 6202 6935
www.ramint.gov.au • ABN 45 852 104 259

Appendix 2: Protective security principles

AGD is responsible for setting the Government's protective security policy. Each Minister is responsible for the protective security of the departments, agencies or bodies within his or her portfolio. Agency heads are responsible to their Minister for creating and maintaining an agency operating environment that:

- safeguards its people and clients from foreseeable risks;
- facilitates the appropriate sharing of official information in order for Government to effectively do business;
- limits the potential for compromise of the confidentiality, integrity and availability of its official information and assets, recognising risks to Government such as those associated with aggregation;
- protects official assets from loss or misuse; and
- supports the continued delivery of the agency's essential business in the face of disruptions caused by all types of hazards.

Agency heads need to understand, prioritise and manage security risks to prevent harm to official resources and disruption to business objectives. Security is not just a cost of doing business, but enables an agency to manage risks that could adversely affect it achieving its objectives. Agencies can only achieve effective protective security if security is part of the agencies' culture, practices and operational plans. Therefore agencies should build protective security into government processes rather than implementing it as an afterthought. Effective protective security and business continuity management underpin organisational resilience.

Agency heads are to ensure that employees and contractors entrusted with their agency's information and assets, or who enter their agency's premises:

- are eligible to have access;
- have had their identity established;
- are suitable to have access; and
- are willing to comply with the Government's policies, standards, protocols and guidelines to safeguard the agency's resources.

Source: AGD, Protective Security Principles, <http://www.protectivesecurity.gov.au/pspf/Pages/Protective-security-principles.aspx>. [Date accessed: 17 April 2014].

Appendix 3: PSPF mandatory requirements

Table A.1: PSPF mandatory requirements in scope for this audit

Reference	Detail
GOV 1	Agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware, and meet the requirements, of the PSPF.
GOV 2	To fulfil their security obligations, agencies must appoint: • a member of the Senior Executive Service as the security executive, responsible for the agency protective security policy and oversight of protective security practices; • an agency security adviser (ASA) responsible for the day-to-day performance of protective security functions; and • an information technology security adviser (ITSA) to advise senior management on the security of the agency's information and communications technology (ICT) systems.
GOV 3	Agencies must ensure that the ASA and ITSA have detailed knowledge of agency-specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.
GOV 4	Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised every two years or sooner when changes in risks and the agency's operating environment dictate.
GOV 5	Agencies must develop their own set of protective security policies and procedures to meet their specific business needs.
GOV 6	Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the *Australian Standards AS/NZS ISO 31000:2009 Risk management—Principles and guidelines* and *HB 167:2006 Security risk management.*
GOV 7	For internal audit and reporting, agencies must: • undertake an annual security assessment against the mandatory requirements detailed within the PSPF; and • report their compliance with the mandatory requirements to the relevant portfolio Minister. The report must: • contain a declaration of compliance by the agency head; and • state any areas of non-compliance, including details on measures taken to lessen identified risks. In addition to their portfolio Minister, agencies must send a copy of their annual report on compliance with the mandatory requirements to: • the Secretary, Attorney-General's Department; and • the Auditor-General.

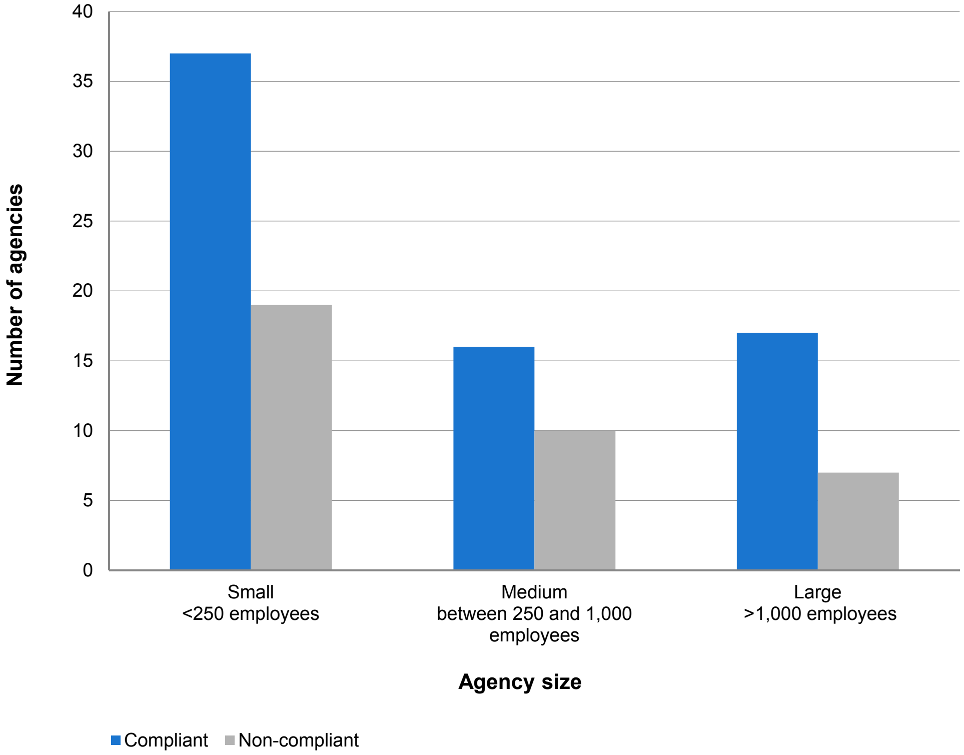
Reference	Detail
GOV 7 (continued)	Agencies must also advise any instances of non-compliance with mandatory requirements to: • the Director, Australian Signals Directorate for matters relating to the *Australian Government Information Security Manual (ISM)*; • the Director-General, Australian Security Intelligence Organisation for matters relating to national security; and • the heads of any agencies whose people, information or assets may be affected by the non-compliance.
GOV 8	Agencies must ensure investigators are appropriately trained and have in place procedures for reporting and investigating security incidents and taking corrective action, in accordance with the provisions of: • Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations; and/or • The Australian Government Investigations Standards.
GOV 12	Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.
PHYSEC 1	Agency heads must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the agency security plan.
PHYSEC 2	Agencies must have in place policies and procedures to: • identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases, agencies may have to extend protection and support to family members and others; • report incidents to management, human resources, security and law enforcement authorities, as appropriate; • provide information, training and counselling to employees; and • maintain thorough records and statements on reported incidents.
PHYSEC 3	Agencies must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.
PHYSEC 4	Agencies must ensure that any proposed physical security measure or activity does not breach relevant employer work health and safety obligations.
PHYSEC 5	Agencies must show a duty of care for the physical safety of those members of the public interacting directly with the Australian Government. Where an agency's function involves providing services, the agency must ensure that clients can transact with the Australian Government with confidence about their physical wellbeing.

Reference	Detail
PHYSEC 6	Agencies must implement a level of physical security measures that minimises or removes the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
PHYSEC 7	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its agencies to implement heightened security levels.

Source: AGD.

Appendix 4: Further analysis of the reported levels of agencies' self-assessed compliance with the 16 mandatory requirements examined in this audit

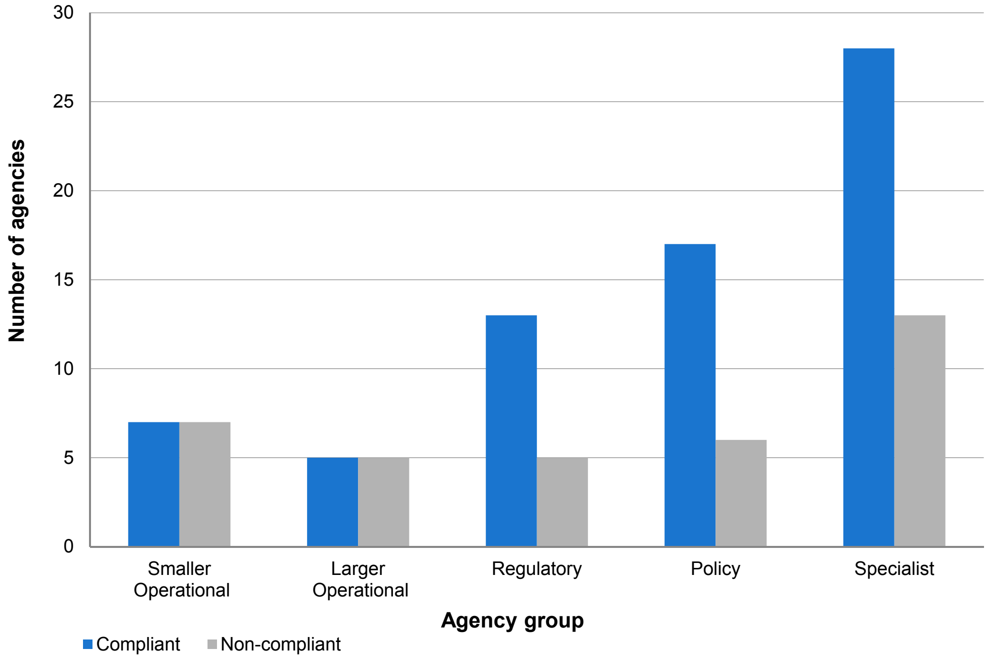
Figure A.1: Reported compliance by agency size



Source: ANAO, based on data from AGD.

Note: An agency is shown as being non-compliant in Figure A.1 if it reported to AGD that it was non-compliant with at least one of the 16 mandatory requirements.

Figure A.2: Reported compliance by agency group



Source: ANAO, based on data from AGD.

Note: An agency is shown as being non-compliant in Figure A.2 if it reported to AGD that it was non-compliant with at least one of the 16 mandatory requirements.

Index

A

Aims of physical security, 29

C

Collaboration, 44, 52

Contracted service providers, 46, 49, 67

H

Heightened threat levels, 54, 58

K

Key security documents, 38, 61–63, 66

Key security roles, 37–38, 46, 67–68

M

Management reports, 41, 52

Mandatory requirements, 28, 39, 78

- ANAO's assessment against, 33, 45, 57, 69
- compliance reporting by agencies, 41–44

Monitoring security risks, 54–55

P

Physical security controls, 54–55, 61, 63–64

Previous audits of protective security, 29

- ANAO's assessment against recommendations, 46, 58, 69

Protective security principles, 27, 77

- governance, 36
- risk management, 49

R

Rating system, 33, 34, 43

Risk-based approach, 50, 68

S

Safety, 29, 30, 46, 49, 58–59

Security

- assurance strategy, 39
- awareness and training, 64–67, 69
- governance, 38, 45, 54
- incidents, 40, 46–47, 66–67
- risk assessment, 52–56, 59, 63
- risk management, 49–51, 53, 56

T

The audited agencies, 31–32

Series Titles

ANAO Audit Report No.1 2013–14
Design and Implementation of the Liveable Cities Program
Department of Infrastructure and Transport

ANAO Audit Report No.2 2013–14
Administration of the Agreements for the Management, Operation and Funding of the Mersey Community Hospital
Department of Health and Ageing
Department of Health and Human Services, Tasmania
Tasmanian Health Organisation – North West

ANAO Audit Report No.3 2013–14
AIR 8000 Phase 2 — C-27J Spartan Battlefield Airlift Aircraft
Department of Defence

ANAO Audit Report No.4 2013–14
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2012 Compliance)
Across Agencies

ANAO Audit Report No.5 2013–14
Administration of the Taxation of Personal Services Income
Australian Taxation Office

ANAO Audit Report No.6 2013–14
Capability Development Reform
Department of Defence

ANAO Audit Report No.7 2013–14
Agency Management of Arrangements to Meet Australia's International Obligations
Across Agencies

ANAO Audit Report No.8 2013–14
The Australian Government Reconstruction Inspectorate's Conduct of Value for Money Reviews of Flood Reconstruction Projects in Queensland
Department of Infrastructure and Regional Development

ANAO Audit Report No.9 2013–14
Determination and Collection of Financial Industry Levies
Australian Prudential Regulation Authority
Department of the Treasury

ANAO Audit Report No.10 2013–14
Torres Strait Regional Authority — Service Delivery
Torres Strait Regional Authority

ANAO Audit Report No.11 2013–14
Delivery of the Filling the Research Gap under the Carbon Farming Futures Program
Department of Agriculture

ANAO Report No.12 2013–14
2012–13 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.13 2013–14
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2013
Across Agencies

ANAO Audit Report No.14 2013–14
Explosive Ordnance and Weapons Security Incident Reporting
Department of Defence

ANAO Audit Report No.15 2013–14
The Indigenous Land Corporation's Administration of the Land Acquisition Program
Indigenous Land Corporation

ANAO Audit Report No.16 2013–14
Administration of the Smart Grid, Smart City Program
Department of the Environment
Department of Industry

ANAO Audit Report No.17 2013–14
Administration of the Strengthening Basin Communities Program
Department of the Environment

ANAO Audit Report No.18 2013–14
Administration of the Improving Water Information Program
Bureau of Meteorology

ANAO Audit Report No.19 2013–14
Management of Complaints and Other Feedback
Australian Taxation Office

ANAO Audit Report No.20 2013–14
Management of the Central Movement Alert List: Follow-on Audit
Department of Immigration and Border Protection

ANAO Report No.21 2013–14
Pilot Project to Audit Key Performance Indicators

ANAO Audit Report No.22 2013–14
Air Warfare Destroyer Program
Department of Defence
Defence Materiel Organisation

ANAO Audit Report No.23 2013–14
Policing at Australian International Airports
Australian Federal Police

ANAO Audit Report No.24 2013–14
Emergency Defence Assistance to the Civil Community
Department of Defence

ANAO Audit Report No.25 2013–14
Management of the Building Better Regional Cities Program
Department of Social Services
Department of the Environment

ANAO Audit Report No.26 2013–14
Medicare Compliance Audits
Department of Human Services

ANAO Audit Report No.27 2013–14
Integrity of Medicare Customer Data
Department of Human Services

ANAO Audit Report No.28 2013–14
Review of Child Support Objections
Department of Human Services
Department of Social Services

ANAO Audit Report No.29 2013–14
Regulation of Commonwealth Radiation and Nuclear Activities
Australian Radiation Protection and Nuclear Safety Agency

ANAO Audit Report No.30 2013–14
Administering the Code of Good Manufacturing Practice for Prescription Medicines
Department of Health

ANAO Audit Report No.31 2013–14
The Australian Electoral Commission's Storage and Transport of Completed Ballot Papers at the September 2013 Federal General Election
Australian Electoral Commission

ANAO Audit Report No.32 2013–14
Delivery of the Hearing Community Service Obligation
Department of Health
Department of Human Services
Australian Hearing Services

ANAO Audit Report No.33 2013–14
Indigenous Employment in Australian Government Entities
Across Agencies

ANAO Audit Report No.34 2013–14
Implementation of ANAO Performance Audit Recommendations
Department of Agriculture
Department of Human Services

ANAO Audit Report No.35 2013–14
Managing Compliance of High Wealth Individuals
Australian Taxation Office

ANAO Audit Report No.36 2013–14
The Administration of the Parliamentary Budget Office
Parliamentary Budget Office

ANAO Audit Report No.37 2013–14
Management of Services Delivered by Job Services Australia
Department of Employment

ANAO Audit Report No.38 2013–14
Establishment and Administration of the National Offshore Petroleum Safety and Environmental Management Authority
National Offshore Petroleum Safety and Environmental Management Authority

ANAO Audit Report No.39 2013–14
Compliance Effectiveness Methodology
Australian Taxation Office

ANAO Audit Report No.40 2013–14
Trials of Intensive Service Delivery
Department of Human Services

ANAO Audit Report No.41 2013–14
Commercialisation Australia Program
Department of Industry

ANAO Audit Report No.42 2013–14
Screening of International Mail
Department of Agriculture
Australian Customs and Border Protection Service

ANAO Audit Report No.43 2013–14
Managing Compliance with Environment Protection and Biodiversity Conservation Act 1999 Conditions of Approval
Department of the Environment

ANAO Audit Report No.44 2013–14
Interim Phase of the Audits of the Financial Statements of Major General Government Sector Agencies for the year ending 30 June 2014
Across Agencies

ANAO Audit Report No.45 2013–14
Initiatives to Support the Delivery of Services to Indigenous Australians
Department of Human Services

ANAO Audit Report No.46 2013–14
Administration of Residential Care Payments
Department of Veterans' Affairs

ANAO Audit Report No.47 2013–14
Managing Conflicts of Interest in FMA Agencies
Across Agencies

ANAO Audit Report No.48 2013–14
Administration of the Australian Business Register
Australian Taxation Office
Australian Securities and Investments Commission
Department of Industry

ANAO Audit Report No.49 2013–14
The Management of Physical Security
Australian Crime Commission
Geoscience Australia
Royal Australian Mint

Better Practice Guides

The following Better Practice Guides are available on the ANAO website:

Administering Regulation	June 2014
Implementing Better Practice Grants Administration	Dec. 2013
Human Resource Management Information Systems: Risks and controls	June 2013
Preparation of Financial Statements by Public Sector Entities	June 2013
Public Sector Internal Audit: An investment in assurance and business improvement	Sept. 2012
Public Sector Environmental Management: Reducing the environmental impacts of public sector operations	Apr. 2012
Developing and Managing Contracts: Getting the right outcome, achieving value for money	Feb. 2012
Public Sector Audit Committees: Independent assurance and advice for chief executives and boards	Aug. 2011
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities: Delivering agreed outcomes through an efficient and optimal asset base	Sept. 2010
Planning and Approving Projects – an Executive Perspective: Setting the foundation for results	June 2010
Innovation in the Public Sector: Enabling better performance, driving new directions	Dec. 2009
SAP ECC 6.0: Security and control	June 2009
Business Continuity Management: Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Fairness and Transparency in Purchasing Decisions: Probity in Australian Government procurement	Aug. 2007
Implementation of Programme and Policy Initiatives: Making implementation matter	Oct. 2006