The Auditor-General
Audit Report No.33 2010–11
Performance Audit

The Protection and Security of Electronic Information Held by Australian Government Agencies

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81178 4

COPYRIGHT INFORMATION

Requests and inquiries concerning reproduction and rights should be addressed to:

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

Or via email:
webmaster@anao.gov.au

Australian National
Audit Office

Canberra ACT
23 March 2011

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit across agencies in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit, and the accompanying brochure, to the Parliament. The report is titled *The Protection and Security of Electronic Information Held by Australian Government Agencies.*

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—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 and financial statement audits 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

Telephone: (02) 6203 7505
Fax: (02) 6203 7519
Email: webmaster@anao.gov.au

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team
Keith Allen
Jillian Blow
Bronwen Jaggers
Wayne Jones
Connal McInnes
Rachel Palmer
Michael White

Contents

Tables

Figures

Abbreviations

AGD	Attorney-General's Department
AOFM	Australian Office of Financial Management
ASA	Agency Security Adviser
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
DRP	Disaster Recovery Plan
DSD	Defence Signals Directorate
ICT	Information and Communication Technology
IDS	Intrusion Detection System
ISM	Information Security Manual
ITSA	Information Technology Security Advisor
PSM	Protective Security Manual
PSPF	Protective Security Policy Framework
SES	Senior Executive Service
SOE	Standard Operating Environment
SOP	Standard Operating Procedures
SRMP	Security Risk Management Plan
SSP	System Security Plan
VPN	Virtual Private Network

Glossary

Cryptography

Cryptography provides a way to distribute or receive information in secret code, so that only the intended parties can read or send it. In an Information and Communication Technology (ICT) environment, cryptography is used to protect against the security risk of information being intercepted, and also to provide proof of the integrity and origin of data.

Disaster Recovery Plan

A Disaster Recovery Plan (DRP) consists of the precautions taken so that the effects of a disaster will be minimised and the organisation will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

Firewall

A firewall is part of a computer system or network that is designed to block unauthorised access while permitting authorised communications. It is a device or set of devices which is configured to permit or deny computer applications based upon a set of rules and other criteria.

Gateway

A Gateway is a network point that acts as an entrance to another network.

Gateway Certification

The Gateway Certification process is designed to assist Australian Government agencies to minimise the risks incurred by connecting their systems to public networks such as the Internet. Gateway Certification entails an independent reviewer validating that the Gateway's safeguards are operating in compliance with an organisation's security policy and Information Security Manual (ISM) requirements.

ICT security policy

An ICT security policy is an integral component of the ICT security control framework. It supports the overall agency security plan by providing a link between the agency's risk management framework and information security policy objectives. An ICT security policy provides the direction and support for the implementation and monitoring of suitable ICT security controls.

Internal network

A network within an organisation.

Internet

The Internet refers to the communications system created by the interconnecting networks of computers around the world.

Operating System

Operating systems are software platforms that manage a computer's functions, and provide a platform on which other programs, called applications, can run.

Patching

A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other program deficiencies and improving the usability or performance of the software. Patch management is the process of using a strategy and plan that details which patches should be applied to which systems, at a specified time.

System Security Plan

An agency System Security Plan provides an overview of the security requirements of a system. It should describe the controls in place or planned, and the responsibilities and expected behaviour of all individuals who access the system.

Summary and Recommendations

Summary

Introduction

1. The Attorney-General has overall policy responsibility for Australian Government[1] protective security arrangements, while agency[2] Chief Executive Officers (CEOs) are responsible for the protective security arrangements within their own organisations. This includes the requirement to 'actively manage security risks associated with electronic data transmission, aggregation and storage'.[3] Given the increasing reliance on Information and Communications Technology (ICT) to deliver services, electronic information security is an increasingly important element of the overall protective security framework.

2. Agency CEOs are required to have in place effective protective security programs that cover requirements associated with:

- each agency's capacity to function;
- maintaining the public's confidence in agencies;
- the safeguarding of official resources and information held on trust; and
- the safety of those employed to carry out the functions of Government and those who are clients of Government.[4]

3. Attacks on agency computer systems can be aimed at damaging critical infrastructure; obtaining access to Government, personal or financial information (for example, identity theft); or making a political point (issue-

[1] For the remainder of this report 'Government' refers to the Australian Government, unless otherwise stated.

[2] In the Government's *Protective Security Policy Framework* (PSPF) an 'agency' is defined as those agencies subject to the *Financial Management and Accountability Act (*FMA Act); those that are subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) and who have received a Ministerial direction to apply the general policies of the Government; and other bodies established for a public purpose under a law of the Commonwealth and other Australian Government agencies, where the body or agency has received a notice from the relevant Minister that the Framework applies to them (Source: Attorney-General's Department, *Protective Security Policy Framework: Securing Government Business*, v.1.1, September 2010). The ANAO has used this definition of 'agency' throughout this report.

[3] The Hon. Robert McClelland MP, Attorney-General, *Directive on the Security of Government Business*, Protective Security Policy Framework, Attorney-General's Department, June 2010.

[4] ibid.

motivated groups).[5] The recent 'Wikileaks' release of Government electronic information has demonstrated the importance of maintaining appropriate protective security frameworks and the risks of failing to adequately protect electronic information.

The Protective Security Policy Framework

4. In June 2010 the Attorney-General announced that the new *Protective Security Policy Framework* (PSPF) had come into effect. The PSPF places an emphasis on the need for agencies to develop an appropriate security culture to securely meet their business needs. The Directive from the Attorney-General to agency CEOs states:

> …agency heads are to ensure that protective security is a part of their agency's culture. A successful culture will effectively balance the competing requirements of limiting access to those that have a genuine 'need to know' with ensuring key business partners receive the information in an appropriate timeframe ('need-to-share').[6]

5. The PSPF outlines four core protective security policies covering Governance, Personnel, Physical and Information security. These four policies incorporate a total of 33 mandatory protective security requirements for agencies,[7] which assist CEOs in developing a security culture within their agency. For example:

- agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware of, and meet the requirements of the PSPF;[8]
- 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;[9] and

[5] Mike Burgess, Deputy Director Cyber and Information Security, Defence Signals Directorate, *Speech to the National Security Australia 2010 Conference*, 26 February 2010.

[6] The Hon. Robert McClelland MP, op. cit.

[7] See Appendix 1 for the full list of the 33 mandatory PSPF requirements.

[8] Attorney-General's Department, *Protective Security Policy Framework*, version 1.1, September 2010, GOV-1.

[9] *Protective Security Policy Framework*, op. cit, GOV-2.

- agencies must develop an agency security plan, protective security policies, procedures and risk assessments that are endorsed by agency heads.[10]

The *Protective Security Manual*

6. The *Protective Security Manual* 2007 (PSM) has been superseded by the PSPF as the source of policy, procedures, and minimum standards for agencies in setting their protective security arrangements. Currently, there is a 12 month transition period between the introduction of the new PSPF and phasing out of the PSM, which is due to be completed by the middle of 2011. AGD has advised that:

> The launch of the Protective Security Policy Framework (PSPF) in June 2010 changed the status of the Protective Security Manual (PSM) to a secondary document, with the PSPF now the prime source on protective security policy expectations. Redevelopment of PSM subject matter into new PSPF protocol, standard, and guidance documents for the new PSPF is underway and expected to be completed by mid 2011. The subject matter in the PSM will be replaced by the new PSPF documents as they are progressively released.[11]

The *Information Security Manual*

7. While the PSPF provides the overarching policy framework, the *Information Security Manual* (ISM 2010[12]) provides the detail on ICT security for agencies to follow. The ISM is prepared by the Defence Signals Directorate (DSD[13]) and its purpose is to 'provide a risk-managed approach to the protection of information and systems in Government'.[14] The ISM sets out the technical measures (controls) for agencies to implement to protect information stored or transmitted via electronic means.

[10] *Protective Security Policy Framework*, op. cit, GOV-4, GOV-5, GOV-6, INFOSEC-2 and PHYSEC-1.

[11] Attorney-General's Department, *PSPF: Transition Interpretation Advice*, 2 December 2010.

[12] The ISM was previously known as the *Australian Government Information and Communications Technology Security Manual,* (ACSI 33), September 2007. The ISM was first released in September 2009 and updated in December 2010.

[13] The Defence Signals Directorate provides the Australian Government with: advice and assistance to federal and state authorities on matters relating to the security and integrity of information; a greater understanding of sophisticated cyber threats; and coordination of and assistance with operational responses to cyber events of national importance across Government and systems of national importance. <http://www.dsd.gov.au/aboutdsd/roleinfosec.htm> [accessed 6 January 2011].

[14] Defence Signals Directorate, *Information Security Manual*, December 2010, p. 1.

Audit objective and scope

8. The objective of the audit was to assess the effectiveness of Australian Government agencies' management and implementation of measures to protect and secure their electronic information, in accordance with Australian Government protective security requirements.[15]

9. The following agencies were selected for inclusion in the audit:

- the Australian Office of Financial Management (AOFM);
- ComSuper;
- Medicare Australia; and
- the Department of the Prime Minister and Cabinet (PM&C).

10. These agencies were selected as they represent a general cross-section of agencies and their associated ICT systems.

11. To address the audit objective, the ANAO examined the extent to which agencies had an effective framework and controls in place across the following four areas: information security framework; network security management; access management; and equipment security.

12. The audit also assessed whether the selected agencies had implemented recommendations from previous ANAO audit reports[16] relating to ICT security management, installation of security patches,[17] review of event logs, and maintenance of ICT documentation. The protection and security of non-electronic information, and Government information held by third parties, such as service providers, was not examined in this audit.

13. The audit was conducted with the support of AGD and the specialist advice of DSD. The ANAO appreciates the time and comments provided by staff at both those agencies throughout the course of the audit.

[15] The objective statement refers to measures to both 'protect' and 'secure' electronic information held by agencies. In this audit, 'protect' refers to measures to safeguard information from external threats, while 'secure' refers to agencies' internal mechanisms to ensure the appropriate safeguarding of information.

[16] ANAO Audit Report No.23 2005–06, *IT Security Management*, and ANAO Audit Report No.45 2005–06, *Internet Security in Australian Government Agencies.*

[17] 'Patches' are pieces of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance of the software. Patch management is the process of using a strategy and plan that details which patches should be applied to which systems, at a specified time.

14. The audit is part of a program of cross-agency performance audits that examines processes supporting the delivery of services by Government agencies. Since 1995 the ANAO has undertaken 11 cross-agency audits on the Government's protective security arrangements. In each of these audit reports the ANAO has encouraged all Government agencies to assess the benefits of the recommendations in light of their own circumstances and practices.

Overall conclusion

15. Delivery of services by Government is reliant on secure and protected ICT systems. Vulnerabilities within ICT systems may allow an attacker to gain access to sensitive information, including information about Government decision making, significant financial transactions, and aggregate personal and financial information. Attackers could also potentially cause disruption to agency services, payments and public information.

16. Agency CEOs are responsible for ensuring that protective security is a part of their agency's culture. Therefore, agencies should build protective security into their business processes and organisation's values. While no ICT system can be completely safe from an intentional or unintentional security breach, agencies should take a risk-based approach in implementing ICT security policies and practices that are based on their assessment of the requirements of the PSPF and the ISM.

17. Overall, the audit concluded that the measures examined in the audited agencies to protect and secure electronic information were generally operating in accordance with Government protective security requirements. The agencies had established information security frameworks; had implemented controls to safeguard information, to protect network infrastructure and prevent and detect unauthorised access to information; and had controls in place to reduce loss, damage or compromise to ICT assets.

18. However, the audit did identify scope for the audited agencies to enhance their security measures in the following key areas:

- information security policies and procedures need to be complete and up-to-date. Some agency policies and procedures were out-of-date, and each agency needed to compile or update their Standard Operating Procedures (SOPs) for ICT security officers. These policies and procedures assist in the consistent implementation of key ICT security measures, controls and practices;

- third-party software applications should be regularly assessed for the availability of patches, and patches applied accordingly, to better protect their security, especially given their known vulnerability to attack. This was an issue identified in two of the four audited agencies;
- administrator accounts and service accounts, which allow a high level of access across ICT systems, should use suitably complex password configurations to reduce the potential for inappropriate access. A password test applied by the ANAO had mixed results, showing weaknesses in passwords for administrator and service accounts in several agencies; and
- emails using public web-based email services[18] should be blocked on agency ICT systems, as these can provide an easily accessible point of entry for an external attack and subject the agency to the potential for intended or unintended information disclosure. Webmail accounts were accessible in one of the audited agencies, and logs showed that some staff were using these accounts on a regular basis.

19. The audit highlights several areas of better practice and makes four recommendations aimed at improving approaches to the protection and security of electronic information. Only the first recommendation applies directly to AOFM. The other three audited agencies each had several issues to address, reflected in the four recommendations. All four of the report's recommendations may also have applicability to other Government agencies.

Key findings by chapter

The Information Security Framework (Chapter 2)

20. Agency CEOs must establish an appropriate and functional information security framework which facilitates the implementation of security measures that match the information's value, classification and sensitivity, and adhere to all legal requirements. More generally, CEOs are also responsible for overseeing the development of an appropriate protective security culture amongst their staff.

[18] This includes the use of unsecured public Internet services such as 'hotmail' or 'gmail' accounts.

21. The PSPF provides an overarching policy framework, including prescribed mandatory requirements, to assist agencies in implementing an information security framework that has regard to principles of accountability, transparency, efficiency and leadership. There are specific requirements regarding oversight arrangements, information security policies and associated plans, including disaster recovery plans.

22. The four agencies subject to audit each had an appropriate information security framework in place. The agencies also had key information security policies and plans. However, some of the policies, and associated procedures, were not regularly updated. These procedures are important to establish that key ICT security measures are consistently implemented and, if necessary, could be undertaken by system users who do not have a strong technical knowledge of the system. The ANAO has recommended that agencies review their information security policies and procedures for completeness and currency.

23. Audited agencies had developed suitable plans to manage a security incident within their agency, and had implemented these plans successfully for recent ICT security incidents. Agencies also had an appropriate program for security training to facilitate staff awareness of information security issues.

Network Security Management (Chapter 3)

24. Network security management refers to the controls implemented by agencies to manage the confidentiality, integrity and accessibility of information as it passes within the agency's network and to, and from, outside networks.

Network security framework

25. The PSPF requires agencies to implement an appropriate network security framework that responds to the business need and level of risk involved. In assessing the network security framework of the audited agencies against the PSPF requirements, the ANAO reviewed key aspects of each agency's ICT system, including: the Intrusion Detection Strategy (IDS); software product patching and the Standard Operating Environment (SOE).

Intrusion Detection Strategy

26. Each audited agency had adequate technical measures for their IDS, in accordance with ISM requirements. Three of the four agencies also had implemented sound procedures for detecting, logging and reviewing intrusions to their ICT systems. However, one agency lacked a robust, documented process for reviewing Internet access logs, thereby increasing the risk of exposing the agency to external intrusion.

Software product patching

27. While the four audited agencies were adequately managing the patching of their core operating systems, two of the agencies had not developed and documented appropriate procedures for managing patches relating to third-party software applications. Patching third-party software is a practice that is recognised by DSD as an effective strategy to mitigate the risk of intrusion into ICT systems. The ANAO has recommended that agencies review their third-party application patching policies, undertake risk assessments on vendor-identified patches and apply patches in a timely manner.

Standard Operating Environment

28. Audited agencies were compliant with the requirements of the ISM regarding the settings applied to SOEs; had implemented procedures regarding the management of relevant changes to network settings; and had up-to-date diagrams showing all connections to the agency network to facilitate the management of system configuration.

Security of information exchange

29. The security of information transmitted within an agency and to external parties is important to agency network security. The ANAO reviewed the cryptographic security and email infrastructure settings of each audited agency to evaluate its security of information exchange settings.

30. Cryptography (the science of writing in a secret code) is a crucial mechanism for ensuring the security of the transmission of agency data. The ISM prescribes that an agency that chooses to use cryptography must comply with approved systems of encryption set out by DSD. Each audited agency used cryptography in a manner compliant with the ISM.

31. Configuring email servers in a secure manner and implementing protective markings to mitigate the risk of malicious emails is a central element of the security of information exchange within, and to and from, an agency. The ISM requires agencies to have specific systems in place to manage the security of email systems. While audited agencies were compliant with the ISM requirements regarding email system security, users could easily circumvent the classification requirements in the email system by attaching a document with a high protective classification marker to an email with a lower protective marker. The risk to agencies is that a classified document may intentionally or unintentionally be emailed to an unsecured or lower-classified network. This is a known risk accepted by most Government agencies in the interests of system functionality. It highlights the need for security awareness and training about the appropriate use of the email classification system.

Implementation of Gateway and network access point security

32. The access point between a secure network and an external environment such as the Internet is an important control for agencies in managing the security of their ICT systems. Agencies need to have appropriate Gateway controls in place on such access points to manage the confidentiality, integrity and availability of agency data. In assessing the access point security controls implemented by agencies, the ANAO considered whether: Gateway configurations were ISM compliant and certified to DSD requirements; content filtering settings were appropriate; and firewalls were appropriately configured.

Gateway configurations

33. The ISM sets out specific technical requirements regarding the configuration of communication paths in and out of internal networks, known as the system's Gateways. There is a certification process for agency Gateways to minimise the security risk faced by agencies when connecting internal networks to external environments. While each agency had appropriate certification for their main Gateways, two agencies were also using uncertified Gateways. The use of uncertified Gateways exposes the agencies to an increased risk of unauthorised access from outside the internal network and is not in accordance with DSD requirements.

Content filtering

34. Audited agencies had appropriate and functional content filtering systems for accessing Internet sites, in accordance with the requirements of the ISM. However, personal email accounts were found to still be accessible in one agency, increasing the risk of external intruder attack for that agency. The ANAO has recommended that agencies reconsider the risks of allowing users access to personal email accounts.

Firewall configurations

35. System firewalls help to protect internal ICT systems from external attack and malicious data originating from the Internet. Audited agencies were using appropriate firewall systems in accordance with ISM requirements.

Access Management (Chapter 4)

36. Agencies are required to develop policies and procedures to manage access to internal ICT networks. The ANAO reviewed user management, including granting and removing user access; agency password policies; and the management of privileged access accounts.

User management

37. Audited agencies had a documented process for granting and removing user access. ANAO analysis of a sample of user commencements and exits found that these documented processes were being followed correctly.

Password policies

38. The ISM prescribes specific controls regarding the selection of passwords in order to mitigate the risk of attempted password compromise. Three of the audited agencies had appropriate password policies, which were reflected in their system configurations. One agency's password settings were not meeting the ISM requirements, however the ANAO was advised this would be corrected with the implementation of a new operating system in February 2011.

39. The ANAO applied a password compromise test designed to assess the strength of users' passwords in the audited agencies. Overall, the test results were mixed, indicating a need for agencies to regularly monitor passwords and ensure users are following password security policies.

Privileged access accounts

40. The password compromise test was also applied to user accounts with privileged access. These types of accounts typically have a high level of system access and would allow an attacker high levels of access to an agency's ICT network, if compromised. In three of the four audited agencies testing indicated that the passwords for privileged access accounts could be compromised.

41. The ANAO has recommended that agencies review the complexity requirements of passwords being used by privileged access account users, to better reflect the risk associated with the level of access these accounts provide.[19]

Equipment Security (Chapter 5)

42. The PSPF and ISM require agencies to implement appropriate levels of physical security to minimise the risk of agency ICT equipment being compromised. The ANAO reviewed agencies' implementation of physical security practices related to ICT equipment.

43. Audited agencies had appropriate management measures in place to minimise the risk of equipment theft or loss, and were compliant with the requirements of the PSPF in relation to the security controls applied to equipment provided by third-party providers.

44. Also, audited agencies had implemented appropriate data protection controls such as the encryption of remotely accessed data to safeguard mobile devices used by agency staff. The agencies also had appropriate policies and controls in place to facilitate remote access for agency staff accessing an internal network externally from the organisation and to monitor usage with anti-virus software in accordance with the ISM requirements.

Summary of agencies' responses

45. The agencies' responses to each recommendation are included in the body of the report, directly following each recommendation. Agencies' general comments on the audit report are below.

[19] It is noted that the ISM prescribes the minimum requirements. Individual agencies should consider their own unique circumstances, and make a determination as to whether more stringent controls are required.

Australian Office of Financial Management

46. The AOFM notes that of the four recommendations, only Recommendation No.1 applies directly to the AOFM. The AOFM agrees to this recommendation.

ComSuper

47. ComSuper welcomes the ANAO report and notes that most of the matters raised will be of interest to all Government agencies. ComSuper notes that its actual protection of electronic information is generally sound, with some differences between ComSuper's arrangements and the prescribed and better practices outlined in the report.

48. ComSuper supports all recommendations in the Report, and commits to remedial action in those particular areas where required.

Medicare Australia

49. Medicare Australia welcomes this report and considers that implementation of the recommendations will enhance the protection and security of electronic information held by Australian Government agencies. Medicare Australia agrees with the recommendations in the report.

The Department of the Prime Minister and Cabinet

50. The Department agrees with all recommendations articulated in the report.

51. As a general comment, the protection and security of electronic information by Australian Government agencies is of increasing importance. Recent events surrounding the unauthorised release of classified US information, as well as the increasing incidents of cyber attacks are a stark reminder of the damage that poor information security can do to Australia's national interests. In that context, [PM&C] would welcome further audits of this nature in the near future.

Recommendations

The recommendations are based on findings from fieldwork at the audited agencies, and are likely to be relevant to other agencies. Therefore, all agencies are encouraged to assess the benefits of implementing these recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by practices already in place.

Recommendation No.1

Para 2.12

To help mitigate the risk of inconsistent application of ICT security measures, the ANAO recommends that agencies review their information security policies and procedures for completeness and currency, and compile or update their Standard Operating Procedures for ICT security officers.

AOFM, ComSuper, Medicare Australia and PM&C: *Agreed.*

Recommendation No.2

Para 3.15

To help manage the risks associated with external attack via third-party applications, the ANAO recommends that agencies review their third-party application patching policies, undertake risk assessments on vendor-identified patches and apply patches in a timely manner.

ComSuper, Medicare Australia and PM&C: *Agreed.*

Recommendation No.3

Para 3.50

To reduce the risk of unauthorised external access to agency systems, the ANAO recommends that, as per *Information Security Manual* requirements, agencies should not allow personnel to send and receive emails on agency ICT systems using public web-based email services. If access to such sites is to be permitted, it should only be on a stand-alone system.

ComSuper, Medicare Australia and PM&C: *Agreed.*

Recommendation No.4

4.17

To reduce the risk of attackers gaining access to privileged access accounts, the ANAO recommends that agencies review the passwords and associated polices that have been set for administrator and service accounts, and where required, set password complexity requirements that are commensurate to the level of risk associated with the level of system privilege.

ComSuper, Medicare Australia and PM&C: *Agreed.*

Audit Findings

1. Introduction

This chapter provides background information about the audit, including an overview of the Australian Government Protective Security Policy Framework and its requirements for information security.

The policy framework and its implementation

1.1 A large proportion of Australian Government[20] business is conducted via electronic means, including information transmission and storage, service delivery, and financial transactions. Accordingly, electronic information security is an increasingly important element of the overall protective security framework.

1.2 The Government requires agency[21] heads to have in place effective protective security programs that cover requirements associated with:

- each agency's capacity to function;
- the public's confidence in the Government and its agencies;
- the safeguarding of official resources and information held on trust; and
- the safety of those employed to carry out the functions of Government and those who are clients of Government.[22]

1.3 Given the reliance on Information and Communications Technology (ICT) to deliver services, agencies are required to 'actively manage security risks associated with electronic data transmission, aggregation and storage'.[23] Attacks on computer systems in both the public and the private sector may be

[20] For the remainder of this report 'Government' refers to the Australian Government, unless otherwise stated.

[21] In the Government's *Protective Security Policy Framework* (PSPF) an 'agency' is defined as those agencies subject to the *Financial Management and Accountability Act (*FMA Act); those that are subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) and who have received a Ministerial direction to apply the general policies of the Government; and other bodies established for a public purpose under a law of the Commonwealth and other Australian Government agencies, where the body or agency has received a notice from the relevant Minister that the Framework applies to them (Source: Attorney-General's Department, *Protective Security Policy Framework: Securing Government Business*, v.1.1, September 2010). The ANAO has used this definition of 'agency' throughout this report.

[22] The Hon. Robert McClelland MP, op. cit.

[23] ibid.

aimed at damaging critical infrastructure; obtaining access to personal and financial information (for example, identity theft); or making a political point (issue-motivated groups).[24] The recent 'Wikileaks' release of Government information has demonstrated the importance of maintaining appropriate protective security frameworks and the risks of failing to adequately protect electronic information.

1.4 Cyber-espionage is another consideration for information security. The Defence Signals Directorate (DSD) has stated that:

> Our national security is under threat from a range of cyber actors. Our adversaries are often well resourced, highly skilled and able to defeat commercially available security solutions.[25]

1.5 The Attorney-General, the Hon Robert McClelland, MP, has policy responsibility for Government protective security arrangements. Under the *Financial Management and Accountability Act 1997* (FMA Act) and the *Commonwealth Authorities and Companies Act 1997* (the CAC Act), agency chief executives are responsible for the protective security arrangements within their own organisations. To provide a coordinated approach to protective security, the Attorney-General's Department (AGD) issues a range of policy guidance and procedures to agencies.

Background to information security policies

1.6 The technical requirements for the protection and security of information were first introduced in the *Australian Government Information and Communications Technology Security Manual* (commonly known as ACSI 33) developed by DSD in 1989. This document has been revised over time and in 2005 was re-released as the *Information Security Manual* (ISM). The ISM sets out the standards which govern the security of ICT systems and was developed to complement the minimum standards and guidance provided in the *Protective Security Manual* (PSM). Further information about the PSM and ISM is provided later in this chapter.

[24] Mike Burgess, op. cit.

[25] Defence Signals Directorate, *Cyber Security Operations Centre* [Internet], available at: <http://www.dsd.gov.au/infosec/csoc.htm> [accessed 5 November 2010].

The Protective Security Policy Framework

1.7 In June 2010 the Attorney-General announced that the new *Protective Security Policy Framework* (PSPF) had come into effect. The PSPF places an emphasis on the need for agencies to develop an appropriate security culture to securely meet their business needs. The Directive from the Attorney-General to agency CEOs states:

> …agency heads are to ensure that protective security is a part of their agency's culture. A successful culture will effectively balance the competing requirements of limiting access to those that have a genuine 'need to know' with ensuring key business partners receive the information in an appropriate timeframe ('need-to-share').[26]

1.8 The PSPF outlines four core protective security policies covering Governance, Personnel, Physical and Information security. These four policies incorporate a total of 33 mandatory protective security requirements for agencies (see Appendix 1 for the full list).

1.9 Table 1.1 below provides an outline of the core policies.

[26] The Hon. Robert McClelland MP, op. cit.

Table 1.1

Protective Security Policy Framework: core policies

PSPF core policy	Detail
Governance - **GOV**	Agencies are to implement protective security governance arrangements including: • using appropriate risk management principles and policies; • monitoring and reviewing their security plan; • annual reporting to the relevant Minister (amongst others) on compliance with the PSPF; • security training for employees; • accountability for outsourced functions; and • investigation of security incidents.
Personnel Security - **PERSEC**	Agencies are to ensure the people they employ are suitable and meet high standards of integrity, honesty and tolerance. Where necessary, people are to be security cleared to the appropriate level.
Physical Security - **PHYSEC**	Agencies are to provide and maintain a safe working environment for their employees, contractors, clients and the public; and a secure physical environment for their official resources.
Information Security - **INFOSEC**[27]	Agencies are to ensure: • they appropriately safeguard all official information to ensure its confidentiality, integrity, and availability by applying safeguards so that: – only authorised people, using approved processes, access information; – information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements; and – information is classified and labelled as required. • information created, stored, processed or transmitted in or over Government Information and Communication Technology (ICT) systems is to be properly managed and protected throughout all phases of a system's life cycle, in accordance with the protocols and guidelines set out in the Protective Security Policy Framework.

Source: Attorney-General's Department, *Securing Government Business: Protective Security Guidance for Executives*, June 2010, p. 3.

The *Protective Security Manual* (PSM) and its replacement

1.10 The PSM (last edition 2007) was previously the source of Government policy, procedures, and minimum standards for agencies in setting their

[27] 'Information' in this context includes both paper and electronic data.

protective security arrangements. A 12-month transition period between the new PSPF and the PSM is planned. AGD has advised:

> The launch of the Protective Security Policy Framework (PSPF) in June 2010 changed the status of the Protective Security Manual (PSM) to a secondary document, with the PSPF now the prime source on protective security policy expectations. Redevelopment of PSM subject matter into new PSPF protocol, standard, and guidance documents for the new PSPF is underway and expected to be completed by mid 2011. The subject matter in the PSM will be replaced by the new PSPF documents as they are progressively released.[28]

1.11 This audit was conducted during the transition phase between the PSM and the PSPF. AGD advised the ANAO that any agency meeting the requirements associated with the PSM would be expected to meet the requirements of the PSPF, as the fundamental requirements associated with security have not changed. Following that advice, the ANAO primarily based the audit criteria on relevant PSPF requirements and some of the key requirements for ICT security contained in the ISM, as outlined below.

The *Information Security Manual*

1.12 The PSPF refers Government agencies to the ISM 2010, prepared by the DSD.[29] The purpose of the ISM is to 'provide a risk managed approach to the protection of information and systems in Government'.[30] The ISM, which continues to apply under the PSPF, details the technical measures (controls) for agencies to implement in order to protect information stored or transmitted via electronic means.

1.13 The ISM contains controls that are categorised as follows:

- **'required' controls**: These controls are mandatory and cannot be risk-managed by anyone other than DSD. These controls relate primarily to the use of high-grade cryptographic equipment and associated plans and systems (for example: agencies are required to contact DSD and

[28] *PSPF: Transition Interpretation Advice*, op. cit.

[29] The Defence Signals Directorate provides the Australian Government with: advice and assistance to federal and state authorities on matters relating to the security and integrity of information; a greater understanding of sophisticated cyber threats; and coordination of and assistance with operation responses to cyber events of national importance across government and systems of national importance. <http://www.dsd.gov.au/aboutdsd/roleinfosec.htm> [accessed 6 January 2011].

[30] Defence Signals Directorate, *Information Security Manual*, December 2010, p. 1.

comply with any requirements for the disposal of high-grade cryptographic equipment[31]);

- **'must' or 'must not' controls**: These controls are considered to be mandatory, except where an agency CEO determines otherwise, on the basis of appropriate risk assessments, mitigation strategies and supporting documentation (for example: agencies must ensure that all systems are awarded accreditation before they are used to process, store or communicate information[32]);
- **'should' or 'should not' controls**: These controls are also considered to be mandatory, however valid reasons to vary from the control could exist in particular circumstances. CEOs (or their delegate) may choose to be non-compliant, on the basis of appropriate risk assessments, mitigation strategies and supporting documentation (for example: agencies should not allow foreign nationals…to have privileged access to systems that process, store or communicate classified information[33]); and
- **'recommended' controls**: Agencies are encouraged to consider implementing recommended controls, taking into account the agency's unique circumstances and having made an informed assessment as to the potential risk to the agency (for example: it is recommended agencies position screens and keyboards so they cannot be seen by unauthorised people[34]).

1.14 The audit examined agencies' compliance with elements of the ISM 'required', 'must/must not' and 'should/should not' controls, together with other elements of the PSPF such as the INFOSEC requirements.

1.15 DSD has also published *Strategies to Mitigate Targeted Cyber Intrusions,* which lists 35 strategies that agencies may implement to prevent targeted cyber intrusions. While these are not mandatory requirements, DSD reports that if agencies had implemented the first four strategies in the list, at least 70

[31] ibid., p. 148.

[32] ibid., p. 46.

[33] ibid., p. 97.

[34] ibid., p. 75.

per cent of the attacks that it responded to in 2009 could have been prevented (this is further discussed in chapters 3 and 4).[35]

About the audit

Audit objective

1.16 This audit is part of a program of cross-agency performance audits that examine processes supporting the delivery of services by Government agencies. Since 1995 the ANAO has undertaken 11 cross-agency audits on the Government's protective security arrangements. In each of these audit reports the ANAO has encouraged all Government agencies to assess the benefits of the recommendations in light of their own circumstances and practices.

1.17 The objective of this audit was to assess the effectiveness of Australian Government agencies' management and implementation measures to protect and secure their electronic information in accordance with Australian Government protective security requirements.[36]

Audit criteria and scope

1.18 The audit assessed the extent to which agencies had effective approaches in the areas outlined in the table below:

[35] The first four strategies are: 1. Patch the operating system and applications that have a corporately manageable auto-update feature. Patch or mitigate serious vulnerabilities within two days. 2. Patch third-party applications. Patch or mitigate serious vulnerabilities within two days. 3. Minimise administrative privileges to only those who need them. 4. Implement application whitelisting to help prevent unapproved programs from running.

Defence Signals Directorate, *Strategies to Mitigate Targeted Cyber Intrusions* [Internet], updated 18 January 2010, available at: <http://www.dsd.gov.au/_lib/pdf_doc/intrusion_mitigations.pdf> [accessed 10 December 2010].

[36] The objective statement refers to measures to both 'protect' and 'secure' electronic information held by agencies. In this audit, 'protect' refers to measures to safeguard information from external threats, while 'secure' refers to agencies' internal mechanisms to ensure the appropriate safeguarding of information.

Table 1.2

Audit objective and criteria

<table>
<tr><td colspan="2"><b>Audit Objective:</b>
<b>To assess the effectiveness of Australian Government agencies' management and implementation measures to protect and secure their electronic information in accordance with Australian Government protective security requirements.</b></td></tr>
<tr><th>High-level criteria</th><th>Question</th></tr>
<tr><td><b>Information security framework</b></td><td>Have agencies established a framework to ensure the implementation and maintenance of effective information security requirements?</td></tr>
<tr><td><b>Network security management</b></td><td>Have agencies implemented adequate technical and non-technical measures to safeguard information stored in and communicated via ICT systems and protect the supporting network infrastructure?</td></tr>
<tr><td><b>Access management</b></td><td>Have agencies implemented adequate technical and non-technical measures to prevent and detect unauthorised access to information systems?</td></tr>
<tr><td><b>Equipment security</b></td><td>Have agencies implemented adequate physical and environmental controls to reduce the risk of loss, damage or compromise of ICT assets and interruption to business activities?</td></tr>
</table>

Source: ANAO.

1.19 The protection and security of non-electronic information, and Government information held by third parties, such as service providers, was not examined in this audit.

Selected agencies

1.20 The following agencies were selected for review:

- the Australian Office of Financial Management (AOFM);
- ComSuper;
- Medicare Australia; and
- the Department of the Prime Minister and Cabinet (PM&C).

1.21 These agencies were selected as they represent a general cross-section of agencies and their associated ICT systems. ComSuper, AOFM and Medicare Australia had also been included in previous ANAO audits on ICT Security Management and Internet Security, and so their efforts to address and implement previous recommendations were also reviewed.

1.22 To minimise the risk of compromising the security of the audited agencies, the audit findings are not reported against each agency, but rather as high-level observations about ICT security issues that may be relevant across the public sector. A detailed set of Issues Papers, containing results pertinent to each individual agency, was provided to allow issues to be addressed.

Audit approach/methodology

1.23 The audit involved interviews of relevant personnel and an examination of related agency documentation; a quantitative and qualitative analysis of the systems, processes and controls the agencies use to protect electronic information; and engagement with external stakeholders including AGD and DSD.

1.24 In particular the audit included a review of:

- the agency's compliance with Government minimum policy standards (the PSPF 33 mandatory requirements and selected 'must' and 'should' statements in the ISM), and any agency-specific policy;
- desktop, server and Gateway standard operating environments, including web and email filtering, management of operating system patches[37] and third-party patch management; and
- the agency's ICT security risk assessments, plans, policies and procedures to ensure they establish controls for securing the agency's Internet services.

1.25 The audit examined agency networks that communicate information up to the level of Highly Protected. [38]

1.26 The audit also assessed whether the selected agencies had implemented recommendations from previous ANAO audit reports relating to ICT security

[37] 'Patches' are pieces of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance of the software. Patch management is the process of using a strategy and plan that details which patches should be applied to which systems, at a specified time.

[38] Under the current *Protective Security Manual*, Australian Government information is categorised under the following classifications: Unclassified; X-in-confidence (e.g. staff, audit, commercial, etc); Protected; Highly Protected; Restricted; Confidential; Secret; and Top Secret. The Restricted, Confidential, Secret and Top Secret classifications are National Security markings and information with one of these markers has more stringent handling, storage and transmission requirements. These classifications are currently (January 2011) under review by AGD.

management, installation of security patches, review of event logs, and maintenance of ICT documentation.[39]

1.27 The ANAO met several times with staff from AGD, as the key policy agency for Government protective security arrangements. The audit was also conducted with the assistance of DSD. DSD's role is to collect and analyse foreign signals intelligence, and provide advice and assistance to Government agencies on information and communications security. DSD's involvement in the audit included assistance with the preparation of the audit work plan, development of the Issues Papers, and the framing of the audit conclusions. The ANAO appreciates the advice and expertise provided by staff at both AGD and DSD during the conduct of the audit.

1.28 The audit was conducted in accordance with the ANAO's auditing standards, at a cost of approximately $475 000. The ANAO used two ICT specialist contractors to assist with technical aspects of audit fieldwork and reporting.

[39] ANAO Audit Report No.23 2005–06, *IT Security Management* and ANAO Audit Report No.45 2005–06, *Internet Security in Australian Government Agencies*.

2. The Information Security Framework

This chapter examines the audited agencies' information security framework and assesses whether they have effective support for the implementation of information security practices.

The importance of an information security framework

2.1 As outlined in chapter 1, agency CEOs are responsible for establishing an appropriate information security culture within their agency, implementing security measures that match the information's value, classification and sensitivity, and adhering to all legal requirements. Therefore, agencies should build protective security into their business processes, rather than implementing it as an afterthought.[40]

2.2 The PSPF provides an overarching policy framework that Government agencies should implement so that they have a program for managing information security risk, and have developed and implemented appropriate policies and plans.

2.3 The PSPF is based on the principles of public sector governance including:

- **accountability**: being answerable for decisions and having meaningful mechanisms in place to ensure the agency adheres to all applicable protective security standards;
- **transparency/openness**: having clear roles and responsibilities for protective security functions and clear procedures for making decisions and exercising authority;
- **efficiency**: ensuring the best use of limited protective security resources to further the aims of the agency, with a commitment to risk-based strategies for improvement; and
- **leadership**: achieving an agency-wide commitment to good protective security performance through leadership from the top.[41]

[40] *Protective Security Policy Framework*, op. cit, section 5.2.

[41] *Protective Security Policy Framework*, op. cit, section 4.

2.4 To guide agencies to achieve this, the PSPF contains 13 'Governance' mandatory requirements, and a number of the INFOSEC requirements address the need for a strong information security framework. These requirements were the basis for the audit criteria regarding each agency's information security framework.

ANAO assessment

2.5 To assess information security frameworks, the ANAO assessed agencies' compliance with the PSPF (sections 4.5 to 4.7; and 5.2) and associated ISM requirements. This included review of documentation, discussion with key staff and the performance of a gap analysis of the ISM 'must' and 'should' requirements against the following key areas:

- oversight and reporting responsibilities for ICT security;
- information and ICT security policies including incident response planning; and
- security awareness and training programs.

Agencies' information security frameworks

Oversight and reporting responsibilities for ICT security

2.6 Under the PSPF, agencies must implement appropriate oversight and reporting responsibilities for protective security that include a member of its Senior Executive Service (SES), an Agency Security Advisor (ASA) with day-to-day responsibility for protective security functions, and an Information Technology Security Adviser (ITSA) to advise senior management on the security of the agency's ICT systems.[42] The aim of these measures is to foster a professional protective security culture, with accountability and transparency for decisions regarding protective security.

2.7 The ANAO found that all four agencies had implemented appropriate oversight responsibilities for their security frameworks. Each agency had CEO and SES oversight of security responsibilities, and at the operational level, the agencies had appointed an ASA and an ITSA.[43]

[42] *Protective Security Policy Framework*, op. cit, GOV-2.

[43] *Information Security Manual*, op. cit, pp. 14-22.

Information and ICT security policies

2.8 Information and ICT security policies and risk plans support the overall information security framework in an agency. The PSPF states that agency CEOs must provide clear direction on information security through the development and implementation of an agency information security policy. The core requirements for an information security framework are outlined in the PSPF and the ISM. Based on these requirements, each agency should have the following key documents:

- an information security policy that:
  - is endorsed by the CEO;
  - details the objectives, scope and approach to the management of information security issues and risks within the agency;
  - identifies information security roles and responsibilities;
  - details the types of information that an employee can disclose as part of his or her job, or the information that they must get permission to disclose;
  - is reviewed and evaluated in line with changes to agency business and information security risks;
  - is consistent with other plans such as the agency security plan and information security risk assessments;
  - addresses issues such as data aggregation and the agency's declassification program;
  - explains the consequences of breaching the policy; and
  - is communicated on an ongoing basis and accessible to all agency employees, and where reasonable and practical is also publicly available.[44]
- ICT-related operational procedures including: Standard Operating Procedures (SOPs) for key systems and roles; Incident Response Plans; access management policies and change control policies.[45]

[44] *Protective Security Policy Framework*, op. cit, INFOSEC 1.

[45] ibid., INFOSEC 4.

2.9 Overall, each agency had the key documents for an effective information security framework, as outlined above. However, a common theme across agencies was that some policies were out-of-date. Further, one agency's policies had never been formally finalised and endorsed by the responsible SES officer/s[46], and other agencies' policies did not precisely meet the requirements of the ISM.

2.10 In all agencies, there were inadequate documented procedures for roles such as the ITSA, IT security officers, and system administrators. Some agencies did not have procedures for these roles, while others had out-of-date policies. SOPs are an important element in ensuring that ICT tasks are undertaken in a consistent manner, and assist in business continuity and disaster recovery planning by spelling out the key tasks that should be undertaken by information security officers. As identified in the ISM:

> SOPS provide a step-by-step guide to undertaking information security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by system users without strong technical knowledge of the system's mechanics.[47]

2.11 Two of the agencies did not have specific Security Risk Management Plans, as required by the ISM. However, risk assessments had been carried out as part of other ICT security planning activities. The ANAO's findings regarding security framework documentation are outlined in Table 2.1 below.

[46] Under the PSPF, a member of the Senior Executive Service must be responsible for the agency protective security policy and oversight of security practices. Security plans must be updated or revised biannually or sooner, when changes in risks and the agency's operating environment dictate. *Protective Security Policy Framework*, op. cit, GOV-2 and GOV-4.

[47] *Information Security Manual*, 2009 edition, section 2.2.36.

Table 2.1

Agencies' information security framework documentation

Agency	Weaknesses in ICT plans/frameworks	PSPF/ISM requirement
Agency A	No Security Risk Management Plan or System Security Plan for a key database managing core business.	PSPF GOV 4, INFOSEC 2 ISM p. 38.
	No SOPs for security officer roles.	PSPF GOV 5, INFOSEC 4 ISM p. 41.
Agency B	No Security Risk Management Plan (although System Security Plans include a risk assessment).	PSPF GOV 4, INFOSEC 2 ISM p. 38.
	No SOPs for security officer roles.	PSPF GOV 5, INFOSEC 4 ISM p. 41.
Agency C	Out-of-date SOPs for security officer roles.	PSPF GOV 5, INFOSEC 4 ISM p. 41.
	IT Security Policy is extremely long and contains verbatim extracts from ISM – not a user-friendly document.	PSPF INFOSEC 1.
Agency D	Out-of-date SOPs for security officer roles.	PSPF GOV 5, INFOSEC 4 ISM p. 41.
	Out-of-date *Incident Response Plan* based on ACSI 33 (2005) requirements.	PSPF INFOSEC 4 ISM p. 44.

Source: ANAO.

Recommendation No.1

2.12 To help mitigate the risk of inconsistent application of ICT security measures, the ANAO recommends that agencies review their information security policies and procedures for completeness and currency, and compile or update their Standard Operating Procedures for ICT security officers.

AOFM response

2.13 Agreed. The AOFM recognises the need to maintain up to date information security policy documentation and standard operating procedures for ICT security officers. The AOFM has commenced a review of its information security policy documentation against the Australian Government Information Security Manual for completeness and currency and will address any deficiencies. It will update this assessment as further applicable guidance documents of the new Protective Security Policy Framework (PSPF) are released by Government.

ComSuper response

2.14 Agreed.

Medicare Australia response

2.15 Agreed. Medicare Australia agrees with this recommendation and will ensure that the policies and procedures identified will be updated and harmonised across the Department of Human Services Portfolio.

Department of the Prime Minister and Cabinet response

2.16 Agreed. The Department continually reviews ICT security documentation and processes and will undertake further changes as new Government policies regarding protective security and information classification are implemented later this year.

Incident Response Planning

2.17 A key component in any overarching information security policy framework is determining possible responses should a security incident occur. The development of an *Incident Response Plan* (IRP) can help agencies manage information security in the event of a security incident. Under the PSPF, agencies are required to 'ensure that they put in place incident management procedures and mechanisms to review violations and to ensure appropriate responses in the event of security incidents, breaches or failures'.[48] The ISM states that an IRP should provide direction on what constitutes an incident, as well as provide steps and procedures for parties to follow to contain, treat and evaluate the incident.[49]

2.18 The ANAO reviewed each agency's IRP and recent incidents to check if there was documentation that showed the nature of the incident, which ICT assets were affected, and the steps taken to address the problem. All four

[48] *Protective Security Policy Framework*, op. cit, INFOSEC 4.

[49] *Information Security Manual,* op. cit, p. 48.

agencies had adequate plans[50] and had followed these plans for recent ICT security incidents.

Security awareness and training programs

2.19 The final key area of an information security framework as identified in the PSPF is to have a training and information program to maintain staff awareness of information security practices. The PSPF mandates this through the requirement for agencies to provide all staff, including contractors, with sufficient security awareness training.

2.20 The ANAO reviewed each agency's security awareness programs and the delivery mechanisms used. Each agency conducts annual 'whole of office' security awareness training, with staff attendance recorded and followed up as necessary. The content of security awareness training courses were not assessed as this matter had been the subject of a recent ANAO audit.[51]

Figure 2.1

Better Practice Example: security awareness training

One audited agency's security awareness training program included the following elements:

- annual security awareness training for all staff–attendance recorded through HR system and non-attendees required to go to alternative sessions at the first opportunity;
- regular security bulletins sent to all staff; and
- a banner message displayed on each computer which users must accept at each logon. The aim of the banner message is to remind staff daily of their security responsibilities.

Source: ANAO.

Reporting requirements for non-compliance

2.21 As noted previously, the reporting requirements for compliance with the Government protective security requirements have changed under the PSPF. During the fieldwork phase of the audit, the ANAO noted instances of

[50] As noted in Table 2.2 above, one plan was significantly out-of-date.

[51] ANAO Audit Report No 25 2009–10 *Security Awareness and Training*.

agencies failing to meet the (then) reporting requirements of the PSM and ISM.[52]

2.22 As highlighted in chapter 1, under the PSPF agencies will need to undertake an annual self-assessment of their compliance against the 33 mandatory requirements of the PSPF. Agencies are encouraged to implement an information security reporting framework that will meet the requirements of the new PSPF.

Conclusion

2.23 Overall, the audited agencies have put into operation effective and appropriately documented information security frameworks that comply with the requirements of the overarching PSPF and the ISM.

2.24 However, agencies need to ensure that their information security polices and associated documents are up-to-date, and regularly reviewed. The review process is particularly important given the rapidly changing nature of information technology equipment and software, and the associated risks with these changes. This issue has been raised in previous ANAO audits on ICT security management.[53]

[52] Under the PSM and ISM, agencies were required to produce 'waiver' documents detailing areas of non-compliance with the PSM or ISM, and lodge these documents with AGD, their Minister, and the Auditor-General.

[53] ANAO Audit Report No. 23, 2005–06, op. cit.

3. Network Security Management

This chapter examines network security practices and summarises the results of technical testing undertaken by the ANAO to determine whether the audited agencies had implemented adequate technical and non-technical measures to safeguard information.

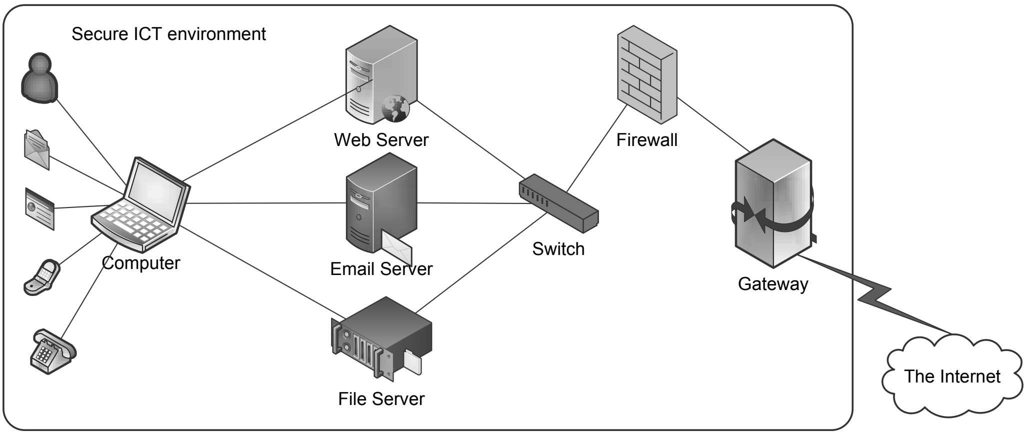
Controls for network security management

3.1 Government agencies are required to implement policies and procedures for the security classification and protective control of information assets (electronic and paper-based) which match their value, importance and sensitivity.[54]

3.2 'Network security management' refers to the controls that are in place to provide the confidentiality, integrity and availability of information as it passes within a network and to and from an outside network (either to other networks within the same organisation or via the Internet to a third party). Figure 3.1 below shows the key elements of an ICT network:

Figure 3.1

Data flow through a network out to the Internet



Source: ANAO.

[54] *Protective Security Policy Framework*, op. cit, INFOSEC 3.

ANAO assessment

3.3 The four agencies included in the audit had different ways of managing and securing their ICT networks. The methods of ICT network management included:

- outsourcing of all ICT services to a single or several external service providers;
- 'piggybacking' an agency's ICT services onto those of another agency in the same portfolio; and
- in-house ICT management with some elements (such as Gateway services) provided externally.

3.4 Whether provided in-house or by external service providers, agencies are responsible for ensuring that their ICT systems meet the PSPF and ISM requirements.[55] To assess the agencies' network security management, the ANAO examined the following key areas:

- network security management practices including cryptographic measures;
- security of information exchange; and
- implementation of Gateway and network access point[56] technical measures.

Agencies' network security management

Network security management practices including cryptographic measures

3.5 The PSPF requires an agency to implement an appropriate network security framework that takes into account the business need and level of risk involved.[57] For this audit, the following areas of network security management were assessed against the ISM requirements:

- Intrusion Detection System (IDS);

[55] *Protective Security Policy Framework*, op. cit, section 5.

[56] Network access points are Internet traffic exchanges with open access policies that support commercial and international traffic.

[57] *Protective Security Policy Framework*, op. cit, sections 5.2 and 5.3.

- software product patching;
- Standard Operating Environment (SOE); and
- configuration management.

Intrusion Detection System

3.6 An IDS can be an effective way of identifying and responding to known attack profiles. An IDS should include technical measures such as content filtering and firewalls (discussed further in this chapter), logging of events, and a regular analysis of logs. IDS procedures should also be audited regularly to ensure they perform as expected.[58]

3.7 In examining the audited agencies' IDS the ANAO was expecting adequate technical measures in line with ISM requirements, and also a sound logging and review process for intrusion detection.

3.8 Standards for ICT systems logging were assessed in a previous ANAO audit report.[59] That audit found that agencies lacked documented processes or procedures for regular monitoring and review of system access logs. This reduced the ability of agencies to monitor and assess the effectiveness of system controls.

3.9 On the whole, each agency had adequate content filtering and firewall settings and three of the four audited agencies also had adequate logging of intrusions and audit procedures for intrusion detection. However, intrusion logs for the fourth agency, which are provided monthly by its service provider, contained a large amount of redundant information, which made the reports unwieldy. Additionally, this agency did not have a robust, documented process for reviewing Internet access logs, which increases the risk of exposing the agency to intrusion from an external attack.

3.10 DSD has identified some more advanced intrusion detection strategy measures in its publication *Strategies to Mitigate Targeted Cyber Intrusions*.[60] At the time of the ANAO's fieldwork (August to October 2010), the audited agencies had not implemented these more advanced strategies (see paragraph 3.57 below).

[58] *Information Security Manual*, op. cit, pp. 242-243.

[59] ANAO Audit Report No.23 2005–06, op. cit, p. 43.

[60] *Strategies to Mitigate Targeted Cyber Intrusions*, op. cit.

Software product patching

3.11 Software, regardless of whether it is operating system-based (for example, Microsoft Windows products) or application-based (software for particular applications such as a publishing program), is subject to vendor-supplied patches being provided on an ongoing basis. The patches may relate to rectification of known security flaws or have the purpose of adding new or updated functionality. The ANAO anticipated agencies would have a regular review process in place to alert them of patches as they become available, and in particular an implementation process to ensure that patches for any known security vulnerabilities are applied as required.[61]

3.12 While all of the agencies were effectively managing the patching of their operating systems, two of the four agencies did not have an effective process for managing patching for third-party applications.[62]

3.13 Patching third-party applications is identified by DSD as the second-most effective strategy that Government agencies can implement to mitigate the risk of targeted intrusion into their ICT networks (the first is to patch the operating system).[63] This is because attackers can exploit known weaknesses in unpatched applications, particularly those that are commonly targeted such as web browsers or productivity applications.

3.14 It is a concern that some agencies are not effectively managing the patching process for third-party applications, as this creates vulnerabilities that may be easily exploited by an external attacker.

Recommendation No.2

3.15 To help manage the risks associated with external attack via third-party applications, the ANAO recommends that agencies review their third-party application patching policies, undertake risk assessments on vendor-identified patches and apply patches in a timely manner.

[61] *Information Security Manual*, op. cit, p. 144. This issue was also raised in ANAO Audit Report No.45 2005–06, op. cit.

[62] Third-party applications are software such as Adobe, ActiveX and web-browsing tools.

[63] *Strategies to Mitigate Targeted Cyber Intrusions*, op. cit.

ComSuper response

3.16 Agreed.

Medicare Australia response

3.17 Agreed. Medicare Australia agrees with this recommendation. We will review our policies and formalise our processes around the management of third-party application vulnerabilities across the Department of Human Services Portfolio.

Department of the Prime Minister and Cabinet response

3.18 Agreed. While critical patches and actions to address security vulnerabilities are undertaken in a timely manner, the Department will take steps to better align and document the patch policy with broader change management processes.

Standard Operating Environment

3.19 A SOE is a standardised build of an operating system and associated software that is deployed on multiple devices. A SOE can be used for servers, workstations, laptops and mobile devices such Personal Digital Assistants (PDAs). Unsecured and uncontrolled SOEs are commonly exploited by attackers to gain unauthorised access to systems.[64] To mitigate the risk of unsecured and uncontrolled SOEs, the ISM has a number of 'must' and 'should' requirements, aimed at securing the software used on workstations and servers.[65]

3.20 Some of the key requirements that should be implemented in the audited agencies' SOEs include:

- removal of redundant software and operating system components;
- disabling of unused or undesired functionality;

[64] *Information Security Manual*, op. cit, pp. 168 and 313.

[65] The ANAO notes that in January 2011 the Australian Government Information Management Office (AGIMO) released the *Whole-of-Government Common Operating Environment Policy*, designed to ensure that agencies' Standard Operating Environments have defined common standards in hardware and software, support the Government's e-Security policy, and improve agencies' ability to share services and applications. The policy was not considered in this audit as it was released after the fieldwork period.

- use of data execution prevention functionality[66], when available;
- access controls to limit system users and programs to the minimum access required (discussed in chapter 4);
- installation of anti-virus software;
- installation of software-based firewalls limiting inbound and outbound network connections (discussed in paragraph 3.54); and
- configuration of either remote logging or the transfer of event logs to a central server.[67]

3.21 The ANAO reviewed the SOE and network management controls for each agency. Each agency had appropriate settings in accordance with the ISM requirements outlined above and a documented change management control process for network changes.

Configuration management

3.22 Configuration management refers to managing how ICT networks are set up, and retaining up-to-date network diagrams. This allows network management decisions to be based on an accurate description of the status of the network.[68] It also reduces the risk that changes to the configuration of the network have unintended consequences to other parts of the network, for example, allowing unauthorised access to information.[69]

3.23 All of the four agencies had up-to-date network diagrams that showed all connections to the network and all communication equipment connections.

Security of information exchange

3.24 Security of information exchange refers specifically to the communication aspects of network security management—that is, the measures an agency needs to implement to protect agency information as it is transmitted either within the organisation or to an external party. In reviewing agencies' controls for security of information exchange the ANAO examined:

[66] Data execution prevention is a security feature in Microsoft Windows operating systems.

[67] *Information Security Manual*, op. cit.

[68] ibid., p. 225.

[69] ibid., pp. 225-226.

- cryptographic security; and
- email infrastructure.

Cryptographic security

3.25 Cryptography is the conversion of data into a secret code, for transmission to another party. Today, most cryptography is digital, and the original text ('plaintext') is turned into a coded equivalent called 'ciphertext', via an encryption algorithm. The ciphertext is decrypted at the receiving end and turned back into plaintext via an encryption algorithm and an encryption key.[70]

3.26 For Government agencies, the decision to use encryption should be a risk-based decision that takes into account the security classification of the data. It is most commonly used for data in transit external to the agency, and for remote access to ICT networks.

3.27 Government agencies may choose to subscribe to FedLink, which is an encryption mechanism supplied by the Department of Finance and Deregulation (Finance) for communications between Government agencies, up to the PROTECTED marking for non-national security classified material, and RESTRICTED for national security classified material. The Government has directed all agencies to use FedLink or an equivalent protection system to protect their data in transit.[71]

3.28 Under the ISM, agencies using cryptography must use algorithms and protocols approved by DSD. Agencies using cryptography in a product for the protection of classified information must ensure that the product has been certified by DSD.[72]

3.29 The ANAO reviewed the cryptographic security controls used by the audited agencies. Each agency subscribes to FedLink and also utilises cryptographic settings for the hard disks in laptops issued to staff, with most also encrypting remote access (including PDAs in some agencies). Overall, the controls were compliant with the ISM requirements.

[70] PC Mag Encyclopedia [Internet], available at: <http://www.pcmag.com/encyclopedia_term/0,2542,t=cryptography> [accessed 7 December 2010].

[71] Department of Finance and Administration, *FedLink* [Internet] available at: <http://www.finance.gov.au/e-government/infrastructure/fedlink/index.html> [accessed 10 December 2010].

[72] *Information Security Manual*, op. cit, p. 202.

Email infrastructure

3.30 Configuring email servers in a secure manner helps to reduce the likelihood of phishing emails[73] and prevent the spread of malicious code.[74] The appropriate management of an agency's network monitoring and email filtering controls is not a new problem for agencies, as they were also recommended as areas requiring improvement in previous ANAO audits.[75]

3.31 Based on ISM requirements, the ANAO anticipated that agencies would have the following controls on email infrastructure:

- a system to block inbound and outbound emails and attachments that contain:
  - malicious code;
  - content in conflict with the agency's email policy;
  - content that cannot be identified; and/or
  - encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source;
- a system to block all emails arriving via an external connection which are purportedly sent from an internal address;
- a system to prevent the sending of email which has no, or an inappropriate, protective marking;
- a system to block outbound and inbound emails which have a protective marking indicating that the content of the email exceeds the classification level of the delivery system;
- a system to ensure automatically forwarded emails are subject to the above controls;

[73] 'Phishing' refers to emails that trick people into giving out their personal, banking or other information; they can also be sent by SMS. These messages seem to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers. The attackers are generally trying to get information such as bank account numbers, passwords and credit card numbers. Source: Scamwatch [Internet], available at: <http://www.scamwatch.gov.au/content/index.phtml/tag/RequestsForYourAccountInformation> [accessed 9 December 2010].

[74] *Information Security Manual*, op. cit, p. 239.

[75] ANAO Audit Report No.23 2005–06, op. cit, p. 41; and ANAO Audit Report No.45 2005–06, op. cit, p.67.

- a system to ensure regular maintenance of email servers; and
- centralised email Gateways—backup or alternative Gateways are often poorly maintained with out-of-date blacklists[76] and content filtering.[77]

3.32 Overall, agencies had implemented appropriate email infrastructure and were meeting the requirements of the ISM, with one exception, outlined below.

3.33 In all audited agencies a user may bypass the classification marking control by providing an incorrect classification to a document attached to the email, because the classifications do not have to match. In a worst-case scenario, this could allow an agency user (or an attacker posing as a user) to email a highly classified document to an external address by attaching it to a lower-classified email.

3.34 The ability to bypass classification markings via an attached document is a known risk that has been accepted by most Government agencies. This is because agencies choose to filter emails using keywords at the email header level, but not at the embedded document level, as the filtering software may generate false 'positive' errors by blocking emails with attachments that may contain legitimate information (for example, a document using the words 'secret' or 'protected', but not actually containing information that is classified SECRET or PROTECTED).

3.35 The ISM does not provide detailed guidance on this issue, stating that agencies must ensure that their users are aware of their email usage policies, and should monitor their email use in accordance with the agency's email use policies. The ISM also states:

> Agencies may choose to monitor compliance with aspects of email usage policies – for example, attempts to send prohibited file types or executables, attempts to send excessively sized attachments or attempts to send security classified information without appropriate protective markings.[78]

[76] A blacklist is a set of inclusive non-accepted items that confirm the item being analysed is not acceptable. It is the opposite of a whitelist which confirms that items are acceptable. *Information Security Manual,* op. cit.

[77] *Information Security Manual*, op. cit, pp. 237–241. The ISM 2010 has several other requirements for email infrastructure controls which were not reviewed by the ANAO, as during the fieldwork stage of the audit the ISM 2009 applied. These new controls cover the blocking of emails that fail Sender Policy Framework checks, and the replacement of active website links within emails with non-active versions.

[78] *Information Security Manual*, op. cit, p. 101.

3.36 The email filtering controls that are in place in each of the audited agencies provide a 'first stage' control. Accordingly, agencies should continue to reinforce the importance of email security practices—particularly the need for staff to check that the protective markings of any documents attached to an email match the email's protective marking—through security policies and regular training.

Implementation of Gateway and network access point security measures

3.37 'Gateway' is a term used to describe the controls used to manage the connection of a secure ICT environment to another environment (usually the Internet). A network access point is a traffic exchange point in the Internet, which controls the flow of information within it (see Figure 3.1). Having appropriate Gateway controls on these access points is critical to maintaining the confidentiality, integrity and availability of data.

3.38 In this audit, the ANAO was expecting that agencies would be able to demonstrate that:

- the Gateway configurations were in compliance with the ISM requirements, and that Gateway certification processes had been followed;
- content filtering settings were appropriate; and
- firewalls were appropriately configured.

Gateway configuration and certification

3.39 The ISM sets out the technical requirements for Gateways used by agencies. Agencies must ensure that Gateways:

- are the only communications paths in and out of internal networks;
- allow only explicitly authorised connections;
- are managed via a secure path isolated from all connected networks (either physically at the Gateway or on a dedicated administration network);
- provide sufficient logging and audit capabilities to detect cyber security incidents and attempted intrusions; and

- provide real-time alerts.[79]

3.40 A Finance-led program is currently working towards reducing the number of Government Internet Gateways in order to improve security, reliability and operational efficiency. This is expected to see a reduction of the 124 Gateways currently in operation, to between four and eight by 2014. Finance states that a reduced number of Gateways will provide improved security through a more consistent approach to Gateway management, accreditation, monitoring and incident response. Gateways will be hosted by selected lead agencies that will, in turn, be allocated client agencies. These agencies will share Gateway services on a cost recovery basis.[80]

3.41 In the meantime, there is a Gateway certification process that agencies submit to, to help minimise the risks incurred in connecting agency networks to a public network. The process provides independent verification that:

- an agency's security policy is being followed;
- appropriate risk management strategies have been implemented;
- countermeasures are operating effectively; and
- residual risk is known.

3.42 Gateway certifications are conducted in accordance with the *Gateway Certification Guide* issued by DSD. Certifications must be undertaken by an assessor who has been accredited with the Infosec Registered Assessor Program (IRAP) run by Standards Australia and DSD. IRAP assessors may provide certification to Gateways up to the PROTECTED level. Agency systems classified higher than this must have a joint assessment undertaken by DSD and an IRAP assessor.[81]

[79] *Information Security Manual*, op. cit, p. 254. The ISM also details some other technical measures that should be applied to Gateways.

[80] Department of Finance and Deregulation, *Incoming Government Brief – AGIMO* 'Lead agency arrangements for a reduced number of Government Internet Gateways' [Internet], 7 September 2010, available at: <http://www.finance.gov.au/publications/IGB/docs/minister-docs/02.2_lead_agency_arrangements_for_a_reduced_number_of_government_internet_gateways.rtf> [accessed 8 December 2010].

[81] Defence Signals Directorate, *Gateway Certification Guide* [Internet], available at: <http://www.dsd.gov.au/infosec/gatewaycertification.htm> [accessed 8 December 2010].

3.43 The ANAO reviewed the Gateway configurations and the Gateway certification status of each agency. A number of issues were identified, as outlined in Table 3.1 below.

Table 3.1

Agencies' Gateway configurations and certifications

Agency	Gateway certification current?	Issues with Gateway configurations
Agency A	Yes	Agency relies on the Gateways provided by its ICT service provider (another portfolio agency). There are no Gateways between the Agency and its ICT service provider. Therefore the ICT service provider personnel with high access privileges may access the Agency network. Agency has documented the risk and it has been accepted by agency executive.
Agency B	Yes	None identified.
Agency C	Yes for main Gateway, No for old Gateway.	The Agency has two Gateway environments: • A 'new' Gateway which is supported by the Agency ICT service provider, and has passed the Gateway Certification process. • An 'old' Gateway is currently being phased out. While still being used for a number of the Agency's normal operations, the Gateway has not been accredited for several years. The ANAO was advised that the old Gateway would be shut down in 2011.
Agency D	Yes for main Gateway (external provider). No for DMZ.[82]	The agency has a DMZ in addition to its main Gateway. The DMZ has not been subject to the Gateway Certification process.

Source: ANAO.

Content filtering controls including web-based email

3.44 It is important for agencies to take a risk-based approach to the types of files (including Internet files) that they allow to be transferred onto their networks. The ISM states that reducing the allowed file types reduces the number of potential vulnerabilities available for an attacker to exploit. In

[82] A Demilitarized Zone (DMZ) is a computer host or small network inserted as a 'neutral zone' between an agency's private network and the outside public network. It prevents outside users from getting direct access to a server that has agency data. However, if the DMZ is not currently certified to the DSD standard, its security cannot be verified.

particular, files that are 'executable'[83], or containing active content embedded in a file, may be harmful if activated by a system user.[84]

3.45 Agencies are expected to have content filtering settings as required by the ISM, and appropriate to the level of risk associated with their ICT networks. This would include an email filtering system (discussed in paragraphs 3.30 to 3.36) and a content filtering system for Internet sites that may include 'blacklisting'. 'Blacklisting' refers to a set of non-accepted items, for example, sites containing adult material or gambling. This is contrasted with 'whitelisting', which refers to activity or content explicitly permitted by the system administrator.

3.46 All agencies generally had appropriate content filtering settings, in accordance with the ISM, with the exception of Internet email ('Webmail'). Webmail systems, such as Gmail, Yahoo and Hotmail, allow email to be delivered directly to a user's desktop, bypassing the Gateway security controls and agency email filtering systems discussed earlier. This creates a risk that a user may download a virus to their desktop, or that a user could send classified information over an insecure network.

3.47 The ISM states that agencies should not allow personnel to send or receive emails using Webmail services.[85] Further, DSD has warned of the increasing sophistication of attackers using 'socially engineered' emails—that is, emails designed to appear legitimate by referring to an individual's interests, friends, or from purportedly legitimate or known address. This type of information can be gathered from social networking Internet sites (such as Facebook).[86] Therefore, it is possible that an attacker could target a person known to be working for a Government agency, sending a socially engineered email to their Webmail account. If the person opened this email from their work desktop, it could allow the attacker to launch a virus or gain unauthorised access to the agency's network.

3.48 Two of the four agencies audited allowed access to Webmail from users' desktops. In one agency, while its ICT security policy stated that users

[83] Executable files cause the computer to perform a set of tasks according to encoded instructions.

[84] *Information Security Manual*, op. cit, p. 262.

[85] *Information Security Manual*, op. cit, p. 100.

[86] Defence Signals Directorate, Cyber Security Operations Centre, *Detecting Socially Engineered Emails,* User Awareness 13/2010, 2 August 2010.

should not use departmental computers to access Webmail, in practice the agency's users were able to access such services. Logs of Internet access in this agency showed that for a two-month period, there were nearly one million 'hits' on Webmail sites (the hit number does not reflect the number of individual accesses to Webmail, as an individual Internet site is typically made up of multiple files, with each file recording a hit once the page is accessed). In the other agency, while the security settings were intended to block Webmail sites, the ANAO was able to access these sites during testing. The agency advised that it has since addressed the problem.

3.49 Due to the risks posed by Webmail access, the ANAO considers that all Government agencies should block access to Webmail accounts, in accordance with the ISM requirements. One option is for agencies to set up a small number of stand-alone computer terminals, where staff can access Webmail (an 'Internet café' approach).

Recommendation No.3

3.50 To reduce the risk of unauthorised external access to agency systems, the ANAO recommends that, as per *Information Security Manual* requirements, agencies should not allow personnel to send and receive emails on agency ICT systems using public web-based email services. If access to such sites is to be permitted, it should only be on a stand-alone system.

ComSuper response

3.51 Agreed. ComSuper has already implemented the practice.

Medicare Australia response

3.52 Agreed. Medicare Australia agrees with this recommendation and has implemented the recommendation through both policy and technical controls but notes that ongoing technological change may change the specifics of the solution to this problem. Medicare Australia will continue to comply with the requirements of the *Information Security Manual.*

Department of the Prime Minister and Cabinet response

3.53 Agreed. Current access arrangements for web based email will cease on 1 July 2011. While access to web based email was in response to business requirements, there were control measures in place. However we accept the threat and risk assessment has changed and access will no longer be permitted from Departmental systems.

Firewall configuration

3.54 A firewall is a device that filters incoming and outgoing data, based on a series of rules.[87] Firewalls are an important element in an agency's overall framework to protect its ICT networks from attacks that originate from the Internet. The ISM states that agencies must use a firewall from DSD's Evaluated Products List,[88] when connecting a network to another network in a different security domain (for example, an IN-CONFIDENCE network to a Public network).

3.55 Firewall configurations and ratings were examined as they applied to the audited agencies' network environments and the Gateway services supplied by external providers. This identified that the firewalls currently being utilised meet the ISM requirements.[89]

Conclusion

3.56 Overall, Government agencies could improve their technical measures to safeguard information stored in ICT systems and protect the supporting network infrastructure. This would include ensuring there are effective software patching policies and procedures in place, Gateways are certified to DSD requirements, and ensuring appropriate email content filtering policies and procedures (particularly with regard to blocking access to Webmail accounts). Highlighted below is a better practice for network security management as observed in one of the audited agencies.

[87] *Information Security Manual*, op. cit, p. 283.

[88] DSD maintains a list of ICT security products certified for use in Australian and New Zealand Government agencies. Further information is available at: <http://www.dsd.gov.au/infosec/epl.htm> [accessed 10 December 2010].

[89] *Information Security Manual*, op. cit, p. 264.

Figure 3.2

Better Practice Example: network security management

Network security management may be improved through the implementation of the following items:

- A documented patching process for the network operating system and third-party applications and monitoring that the processes are implemented.
- SOE and configuration management practices that meet the requirements of the ISM.
- Email filtering software that blocks delivery of suspicious emails and prevents sending unmarked or inappropriately marked emails (with the exception of attached documents, as discussed earlier in this chapter).
- Content filtering software that blocks access to Internet sites that are inappropriate for work use or may be high risk for malicious content, such as those with adult content, gambling, chatrooms, dating sites, criminal or terrorist information, Webmail, music downloads and SPAM.
- A documented process for the maintenance and regular review of Internet access and Intrusion Detection logs, and monitoring that processes are being followed.
- Gateways and firewalls that comply with ISM requirements and the Gateways have a current Certification.
- An ICT *Personal Responsibilities Guide* which outlines the agency's expectations of staff regarding use of ICT equipment and the network.
- A detailed ICT security training course which highlights the risks associated with suspicious emails and Internet sites (including socially engineered emails) and what users should do if they receive such emails or download suspicious files from the Internet.

Source: ANAO.

3.57 Additionally, as noted in paragraphs 1.15 and 3.10, DSD has released its *Strategies to Mitigate Targeted Cyber Intrusions* document, which outlines the measures agencies may implement to prevent targeted cyber intrusions. DSD reports that at least 70 per cent of the attacks that it responded to in 2009 could have been prevented if agencies had implemented the first four strategies listed in the document. The first four strategies are:

- patch the operating system and applications that have a corporately manageable auto-update feature. Patch or mitigate serious vulnerabilities within two days;

- patch third-party applications, for example PDF viewer, ActiveX objects and other web browser plugins. Patch or mitigate serious vulnerabilities within two days;
- minimise administrative privileges to only users who need them. Such users should use a separate unprivileged account for email and web browsing; and
- implement application whitelisting to help prevent unapproved programs from running.[90]

3.58 Based on DSD advice, the ANAO suggests that agencies should implement the top four mitigation strategies, and consider further implementation of the other strategies based on their assessment of their own agency's information security risks.

[90] *Strategies to Mitigate Targeted Cyber Intrusions*, op. cit.

4. Access Management

This chapter examines the audited agencies' access management procedures to assess whether they have implemented adequate technical and non-technical measures to prevent and detect unauthorised access to information systems.

Access to information systems

4.1 A critical element of an agency's information security framework is the robustness of the policies and procedures used to control how users access its information systems and the information contained within them. Controlling and monitoring system access through the use of passwords, for example, can help to provide greater assurance to the system owner about who is accessing the system and for what purpose.

4.2 The PSPF requires that agencies have control measures based on the business owner requirements and assessed and accepted risks for controlling access to information, ICT systems, networks and applications.[91] The ISM also provides more detailed guidance on access management controls such as password complexity and administrator access.

ANAO assessment

4.3 Agency access management policies and procedures were assessed through examination of documentation, discussion with key staff and the performance of a gap analysis of the ISM 'must/must not' and 'should/should not' requirements against the following key areas:

- user access management, including systems for granting user access and removing user access;
- passwords policy and practice; and
- management of system administrator privileges.

[91] *Protective Security Policy Framework*, INFOSEC 5.

Agencies' user access management

New users and exiting users

4.4 Each agency's access management framework was reviewed to see how new users are given access to the ICT system. Agencies are required to have a documented procedure for giving a new user access to the ICT system, and for removing users[92] once they leave the agency's employment. Agencies are also required to remove a system user account when it is no longer required to prevent other users from accessing old accounts, and to reduce the number of accounts that an attacker can target.[93]

4.5 Each agency had documented processes for allowing a new user access to the ICT system and removing users who were leaving the agency, including approval by a supervisor and, for new users, issue of a password that has to be changed on initial logon. A sample of user commencements and exits in each agency was reviewed and it was established that the processes were being followed satisfactorily.

Password integrity

4.6 An assessment was conducted of password selection policies and password management practices implemented by the audited agencies. Password policies and practices are aimed at preventing ICT systems authentication information being easily undermined by brute force attack.[94] Software designed to 'crack' passwords is freely available on the Internet, and attackers may use this software in an attempt to gain access to an agency ICT system. The ISM states that a simple six-letter password can be cracked in minutes. Passwords with at least seven characters, with a combination of upper and lower case letters, numbers and special characters, have a much greater resistance to such attacks.[95] Therefore it is critical that agencies have an appropriate password policy that is consistently implemented, in order to manage the risk of attack from an external source.

[92] Some systems, for example SAP business management systems, require user accounts to be disabled not deleted, as the account is required for audit trail purposes.

[93] *Information Security Manual*, op. cit, p.199.

[94] Brute force attack tests run a guess of password combinations including symbols.

[95] *Information Security Manual*, op. cit, p. 192.

4.7 Overall, agencies' password policies were compliant with the ISM requirements. One agency did not meet the ISM minimum requirements for passwords to have at least seven characters, and to include complexity such as a mix of upper and lower case letters, numbers or some symbols. The ANAO was advised that this problem would be rectified in a planned move to a new operating system in February 2011.

ANAO password analysis exercise

4.8 As well as assessing agencies' password policies, it is important to also test the implementation of these policies, to ensure the integrity of password controls. To test the robustness of agencies' compliance with the password complexity rules and the effectiveness of security awareness training for users, the ANAO, with agreement from each agency, performed a password analysis exercise using password analysis software.[96] This involved obtaining a download of a password file from a nominated server and using the software to perform a series of tests designed to assess the strength of users' passwords, including:

- passwords used by 'ordinary' system users (that is, those without a high level of system access privileges);
- passwords selected by the Helpdesks when resetting a user's password;
- service account passwords which never expire; and
- administrator account passwords.

4.9 Service accounts are system accounts set up specifically to allow applications to run their processes in the background without user intervention. They are typically set up with one-time passwords that never expire, and generally have high system access privileges.

4.10 Administrator accounts typically have wide-ranging access privileges. The ISM states that such 'privileged users' can have the capability to modify system configurations, account privileges, audit logs, data files or applications.[97] Therefore these accounts are highly desirable for an attacker to access.

[96] Under normal circumstances, users in each agency cannot load unapproved software onto their ICT environments.

[97] *Information Security Manual*, op. cit, p. 310.

4.11 While all the audited agencies' systems settings met the complexity requirements of the ISM (with the exception noted in paragraph 4.7 above), better practice, achieved mainly through user awareness, is that users choose passwords that are suitably complex, that is, not just a dictionary word with a capital letter and a number (for example Holiday1).[98] This is particularly the case for service accounts and administrator accounts.

4.12 While the ISM does not prescribe more complex password requirements for administrator or service accounts than for normal system users, under a risk-based framework better practice would suggest that agencies should consider the merits of making these passwords more robust.

Purpose of the test

4.13 The purpose of the exercise was to gain assurance over the integrity of agencies' password configuration and users' understanding of the need to select a suitably complex password. The test approach used a combination of dictionary, hybrid (dictionary plus numbers) and 'brute force' analysis techniques.[99] The tests were run for only one hour as this is a sufficient period of time to validate the password integrity for the first two tests in particular. It is also considered sufficient time to provide a snapshot of password integrity using the more intensive 'brute force' test.

Test results

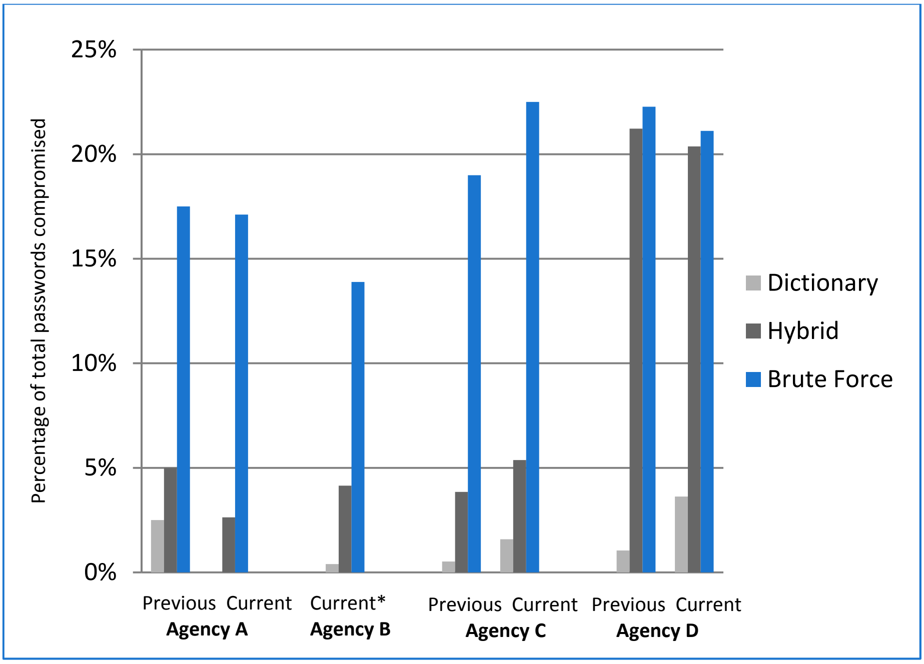
4.14 The test results, detailed in Figure 4.1, show a low rate of compromise of agency passwords in the dictionary and hybrid tests. The 'brute force' attack, however, had a higher success rate. Some standard security settings such as a lock-out after a number of unsuccessful password attempts would mitigate some of the risk associated with a brute force attack. The results of the password analysis exercise for all four agencies are outlined in Figure 4.1 below.

[98] Some useful advice on choosing a good password is available from AusCERT: <http://www.auscert.org/render.html?it=2260> [accessed 23 December 2010].

[99] The dictionary test runs 3000 common words. The hybrid test runs the dictionary test plus numbers. The 'brute force' test runs a guess of password combinations including symbols, and if left to run indefinitely, would be highly likely to expose password weaknesses in totality.

Figure 4.1

Results of password analysis exercise, all audited agencies



* Only current passwords were available from this agency.

Source: ANAO analysis.

4.15 For each agency, the dictionary and hybrid tests were not very successful (at less than five per cent each), while the 'brute force' test resulted in around 20 per cent of passwords being compromised in each agency. It is difficult to 'benchmark' such a result. In an ideal world, there would be little or no compromise of passwords using such a test, however, advice to the ANAO is that a 20 per cent result compares reasonably favourably with some private sector and State government agencies.

4.16 Of more concern was that in three of the four agencies audited, the test compromised some administrator and/or service account passwords. As outlined above, these types of accounts have a high level of access to agencies' ICT systems. If an attacker managed to gain access to an agency ICT system by cracking an administrator or service account password, there could be serious consequences for that agency's security.

Recommendation No.4

4.17 To reduce the risk of attackers gaining access to privileged access accounts, the ANAO recommends that agencies review the passwords and associated polices that have been set for administrator and service accounts, and where required, set password complexity requirements that are commensurate to the level of risk associated with the level of system privilege.

ComSuper response

4.18 Agreed.

Medicare Australia response

4.19 Agreed. Medicare Australia agrees with this recommendation and will coordinate within the Department of Human Services Portfolio to ensure the recommendation is implemented.

Department of the Prime Minister and Cabinet response

4.20 Agreed. Review of privileged access accounts is regularly undertaken, and furthermore, the Department will continue to limit the number of accounts as operational requirements dictate.

Potential use of password integrity exercises

4.21 A password integrity exercise, such as the test conducted for this audit, provides useful information to agencies about potential password weaknesses, particularly in administrator and service accounts. If an agency conducted carefully controlled password integrity exercises on a regular basis, spikes in password compromise may indicate a need for user training or refresher courses in how to select a suitable password, appropriate for the user's level of system access.

Management of system administrator privileges

4.22 As outlined in paragraph 4.10, a system administrator is a person employed to maintain and manage a computer system and/or network. Their duties are wide-ranging and usually include the installation, support and maintenance of servers/computer systems, and planning for and responding to service outages and other problems. In order to perform these functions they generally require 'full' access privileges for the network services they maintain and operate.

4.23 As DSD notes, 'an attacker who gains access to a system with system administrator privileges will have the ability to not only access information but to control that system completely'.[100]

4.24 DSD's *Strategies to Mitigate Targeted Cyber Intrusions* states that controlling administrator privileges is the third most effective strategy that Government agencies can implement to mitigate the risk of intrusion on their ICT systems. The document says that agencies should 'minimise administrative privileges to only users who need them. Such users should use a separate unprivileged account for email and Web browsing'.[101]

4.25 While the PSPF provides high-level guidance on system access[102], the ISM provides detailed guidance on the requirements for administrator (described in the ISM as 'privileged') access. As a general rule, agencies should limit system access to a need-to-know basis, and provide users with the least amount of privileges needed to undertake their duties, balanced with the 'need to share' in order to conduct agency business in an effective manner.[103] The ISM describes 'privileged' access as that which can give a user one or more of the following:

- the ability to change key system configurations;
- the ability to change control parameters;
- access to audit and security monitoring information;
- the ability to circumvent security measures;
- access to data, files and accounts used by other system users, including backups and media; and
- special access for troubleshooting the system.[104]

[100] *Information Security Manual*, op. cit, p. 213.

[101] *Strategies to Mitigate Targeted Cyber Intrusions*, op. cit.

[102] *Protective Security Policy Framework*, INFOSEC 5.

[103] *Information Security Manual*, op. cit, p. 92.

[104] *Information Security Manual*, op. cit, p. 96.

4.26 Based on the ISM requirements, agencies should have systems in place to ensure:

- that privileged accounts were kept to a minimum;
- that the use of privileged accounts was controlled and accountable;
- that administrators were assigned an individual account for the performance of their tasks, and that these accounts would be used for administrative work only (that is, not for other tasks like email or Internet browsing); and
- that privileged users had appropriate classification clearances relevant to the systems that they would be dealing with.

4.27 All agencies were found to have sufficient clearance requirements for users with privileged access. In three of the four agencies, system administrators have dual logons which allow them to use the system with 'normal' access levels or 'privileged' access. The ISM states that agencies should allow the use of privileged accounts for system administrator tasks only, and other activities such as Internet browsing or sending emails should be performed using 'normal' access accounts.[105] The agency that did not have dual logons for its system administrators stated that it intended to introduce this control for system administrators to ensure it meets this ISM requirement.

Figure 4.2

Better Practice Example: controls for system access

One agency had a better practice example for re-validation of users' system access. This involved:

For 'privileged' users with a high level of system access, a three-monthly review, via an automatically generated email from the ICT service provider listing all users with privileged access. The email is delivered to the manager who originally approved each user's privileged access. The manager must then confirm or update the details and send it back to the ICT service provider.

A similar process is conducted at least every six months for 'normal' users.

Source: ANAO.

[105] *Information Security Manual*, op. cit, p. 96.

Conclusion

4.28 Overall, the audited agencies were generally compliant with the relevant PSPF and ISM requirements, as no critical issues regarding the agencies' access management were identified. However, the ANAO recommends that agencies review the integrity of their administrator account passwords, as included in DSD's *Strategies to Mitigate Targeted Cyber Intrusions*.

5. Equipment Security

This chapter assesses the extent to which the audited agencies had implemented effective controls to protect ICT assets.

Protecting ICT equipment and remote access

5.1 The protection of ICT equipment, including the information held and transferred via that equipment, is a significant security risk to be managed by all agencies. The adequacy of an agency's physical security framework is therefore key to ensuring that these assets are protected from accidental or deliberate damage or loss.

5.2 The importance of appropriately securing data on laptops and other portable devices was recently highlighted in an incident in the UK where a laptop purchased from eBay contained highly sensitive military information.[106] In this instance the data files had not been wiped from the system, encrypted, or subject to any password controls.

ANAO assessment

5.3 Elements relating to the audited agencies' physical security were assessed, as they related to the protection of ICT equipment and management of contract/third-party requirements. The PSPF requires an agency to implement an appropriate level of physical security measures to minimise the risk of ICT equipment and information being compromised either accidentally or deliberately.[107] Further guidance is also provided in the ISM.[108]

5.4 It was expected that agencies had appropriate security practices for the following areas:

- on-site equipment such as computers and servers;
- mobile devices such as laptops and personal digital assistants;

[106] NewsCore, '*Laptop bought on eBay contains details of every UK soldier serving in Afghanistan province' [Internet]*, 12 November 2010, news.com.au, available at <http://www.news.com.au/technology/laptop-bought-on-ebay-contains-details-of-every-uk-soldier-serving-in-afghanistan-province/story-e6frfro0-1225952465394> [accessed 12 November 2010].

[107] *Protective Security Policy Framework,* op. cit, p. 35.

[108] *Information Security Manual*, op. cit, p. 74 onwards.

- security requirements when working from home and accessing ICT systems from home computers;
- equipment provided off-site by external service providers (for example, server rooms); and
- compliance with mandated controls such as DSD requirements for storing SECRET or TOP SECRET materials.

Agencies' measures for equipment security and remote access

Securing on-site resources

5.5 On-site computing resources include desktop computers and associated equipment, laptops used predominantly in agency offices, computer servers, cabling and other hardware.

5.6 The loss or theft of agencies' computing equipment, particularly laptop computers, was highlighted in a 2003 inquiry by the Joint Committee of Public Accounts and Audit. That inquiry found that in the five years from 1998–2003, more than 1000 Government laptops, 290 desktop computers and 175 other pieces of computer hardware were either lost or stolen.[109] Recent audits for several State governments have highlighted this as an ongoing concern.[110]

5.7 An examination of each agency's security for on-site computing resources was conducted via discussions with key staff, documentation review, and a walk-through of sites including server rooms. Two of the agencies had recently commissioned a security review conducted by an external organisation, and the reviews had highlighted some issues for the agencies to address. Taking into account the agencies' efforts to address the issues highlighted in the security reviews, each of the four agencies had taken appropriate steps to manage physical security measures for their on-site computing equipment.

[109] Joint Committee of Public Accounts and Audit, *Inquiry into the Management and Integrity of Electronic Information in the Commonwealth*, Parliament of Australia, April 2004.

[110] For example, Western Australia Auditor-General's Report, *Information Systems Audit Report*, Report 2: March 2010, Parliament of Western Australia.

Security of mobile devices

5.8 In recent years, the term 'mobile devices' has included items such as laptops, mobile phones, personal digital assistants such as Blackberrys, and portable data storage such as thumbdrives. However the emergence of new technologies means that Government employees are increasingly likely to also use devices such as smartphones, netbooks and tablet computers to access their agency's ICT systems or communicate on behalf of their agency.

5.9 The risk associated with such use is that small devices are more easily lost or stolen—thereby resulting in a 'data spill',[111] information on a screen may be observed by a third party, or conversations may be overheard in a public arena. The ISM requires agencies to develop a policy governing the use of mobile devices. TOP SECRET information must not be stored or transmitted on mobile devices, unless explicitly approved by DSD to do so.[112]

5.10 A review was conducted to see if each agency had a policy governing the use of mobile devices and connection to the ICT system from an external source, and that the policy was being appropriately implemented.

5.11 Each of the audited agencies had a policy for the use of mobile devices. Each agency issues laptops and portable mobile devices to some staff, to enable them to work from home or other locations. As outlined in chapter 3, each agency encrypts the hard disks in the laptops to at least the EAL 2 standard.[113] The portable devices are also appropriately encrypted. In this audit the security of portable data storage devices (for example, thumbdrives) was not reviewed, but it is noted that given their small size, these devices may be easily misplaced or stolen.

5.12 While the ISM sets out a number of technical requirements for the use and configuration of mobile devices, given the increasing types of mobile devices and their use by Government employees, there is also a strong onus on employees to take responsibility for the security of their mobile devices and their actions while using them, particularly in public. This underlines the importance of regular ICT security awareness training that is relevant to the

[111] A 'data spill' is a term commonly used to describe the unintentional release of secure information to an un-trusted environment.

[112] *Information Security Manual*, op. cit, p. 269.

[113] EAL 2 and EAL 4 are encryption levels designated by DSD for the protection of agency devices. The levels vary depending on the security classification level of the device or the information it supports.

work of the agency, its risk profile, and its use of ICT equipment such as mobile devices.

Working from home

5.13 It is increasingly common for Government agency employees to work from home (in either permanent or ad-hoc arrangements), using their own computer to access an agency's ICT system, or an agency-issued laptop.[114]

5.14 The ISM states that working from home arrangements must meet the minimum physical security requirements of the PSPF. This includes ensuring there are adequate storage arrangements for devices when they are not in use. Agencies may be responsible for modifying a home environment to ensure that the minimum requirements are met.[115]

5.15 The ANAO reviewed each agency's working from home policy and a sample of assessments that had been undertaken in employee's homes. This review found that each agency was complying with the ISM requirements.

5.16 The ability to log into an agency's network from an outside location is known as a Remote Access Solution. The ISM requires that each remote connection is authenticated before access to an agency system is permitted. Both the device and the user seeking access should be authenticated.[116] The ISM recommends that agencies do not allow the use of privileged access remotely.

5.17 The ANAO found that each agency allowed staff to access their ICT system through an agency-issued laptop, using a secure Internet access solution and an appropriate authentication system. Two of the agencies allowed home computers to access the system via a Virtual Private Network (VPN) solution[117], but the access was limited to 'view', with print and write access disabled. All remote connections are also monitored with anti-virus software.

[114] Australian Public Service Commission, *Submission* to the Productivity Commission's public inquiry into Paid Maternity, Paternity and Parental Leave, June 2008, available at: <http://www.pc.gov.au/__data/assets/pdf_file/0009/80739/sub098.pdf> [accessed 15 December 2010].

[115] *Information Security Manual*, op. cit, p. 275.

[116] *Information Security Manual*, op. cit, p. 196.

[117] A VPN is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to the organisation's network.

5.18 Mobile computing is a rapidly changing environment, and several agencies had recently reviewed their policies and practices for security of off-site equipment. All agencies are encouraged to have a regular review framework for ICT equipment security policy and practice.

Equipment provided by third parties

5.19 All of the audited agencies used services and equipment provided by a third party as part of their ICT framework. Formal contractual arrangements govern the provision of these services.

5.20 The ANAO reviewed relevant third party-contracts and IRAP assessments[118] to establish the inclusion of requirements for the security of off-site equipment (such as servers). The review included a physical examination of third-party premises. The physical security controls, contract requirements and contract monitoring processes observed by the ANAO were considered sufficient to meet the PSPF mandatory requirements. The PSPF framework will include a more detailed *Physical Security Protocol* (replacing the PSM), due to be released in 2011. Agencies will need to review their current security arrangements in light of the more detailed guidance to be provided in the PSPF.

Conclusion

5.21 Overall, the audited agencies have taken appropriate steps to manage physical security measures to reduce the risk of loss, damage or compromise of ICT assets and interruption to business activities for those components that were tested.

Ian McPhee

Auditor-General

Canberra ACT

23 March 2011

[118] See Chapter 3.

Appendices

Appendix 1: Protective Security Policy Framework: 33 Mandatory Requirements

Table A 1

PSPF mandatory requirements

Mandatory Requirements – summary table		
1	GOV-1	Agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware of, and meet the requirements of this Framework.
2	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 Communications Technology (ICT) systems.
3	GOV-3	Agencies must ensure that the agency security adviser (ASA) and information technology security adviser (ITSA) have detailed knowledge of agency-specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.
4	GOV-4	Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised biannually or sooner when changes in risks and the agency's operating environment dictate.
5	GOV-5	Agencies must develop their own set of protective security policies and procedures to meet their specific business needs.
6	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 Standard for Risk Management AS/NZS ISO 31000:2009 and the Australian Standards HB 167:2006 Security risk management.

Mandatory Requirements – summary table		
7	GOV-7	For internal audit and reporting, agencies must: • undertake an annual security assessment against the mandatory requirements detailed within this Framework, 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. Agencies must also advise any non-compliance with mandatory requirements to: • the Director, Defence Signals Directorate for matters relating to the Australian Government ICT 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.
8	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 Guidelines on Security incidents and Investigations, and/or • The Australian Government Investigations Standards.
9	GOV- 9	Agencies must give all employees, including contractors, guidance on Sections 70 and 79 of the Crimes Act 1914, section 91.1 of the Criminal Code 1995, the Freedom of Information Act 1982 and the Information Privacy Principles contained in the Privacy Act 1988 including how this legislation relates to their role.
10	GOV-10	Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Australia is a party.
11	GOV-11	Agencies must establish a business continuity management (BCM) program to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment.
12	GOV-12	Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.

Mandatory Requirements – summary table		
13	GOV-13	The following agencies must comply with the *Commonwealth Fraud Control Guidelines – May 2002:* • all agencies that are subject to the Financial Management and Accountability Act 1997, and • Commonwealth Authorities and Companies Act 1997 agencies that are at least 50% budget funded for their operating costs.
14	PERSEC 1	Agencies must ensure that Australian Government employees, contractors and temporary staff who require ongoing access to Australian Government information and resources: • 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 that safeguard that agency's resources (people, information and assets) from harm. Access to higher levels of classified resources is dependent upon the granting of the requisite security clearance.
15	PERSEC 2	Agencies must, as part of their risk management approach to protective security, identify designated security assessed positions (DSAPs) within their organisation that require access to CONFIDENTIAL, SECRET and TOP SECRET assets and information. Agencies must ensure that security vetting is only applied where it is necessary.
16	PERSEC 3	Agencies must maintain a DSAP register.
17	PERSEC 4	Security clearances must be sponsored by an Australian Government agency. Security clearances are not available on demand or on a speculative basis.
18	PERSEC 5	All Government agencies must follow the Australian Government Personnel Security Protocol for personnel security as contained in supplementary material within the Protective Security Policy Framework. Only the Australian Government Security Vetting Agency and exempt agencies can grant, continue, deny, revoke or vary a security clearance. Exempt agencies can only issue clearances for their own agency.
19	PERSEC 6	Agencies must have in place personnel security aftercare arrangements, including the requirement for individuals holding security clearances to advise the AGSVA or the relevant exempt agency of any significant change in personal circumstance that may impact on their continuing suitability to access security classified resources.
20	INFOSEC 1	Agency heads must provide clear direction on information security through the development and implementation of an agency information security policy and an agency information security plan.
21	INFOSEC 2	Each agency must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency's information environment.

Mandatory Requirements – summary table		
22	INFOSEC 3	Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats) which match their value, importance and sensitivity.
23	INFOSEC 4	Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security.
24	INFOSEC 5	Agencies must have in place control measures based on business owner requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Agency access control rules must be consistent with agency business requirements and information classification as well as legal obligations.
25	INFOSEC 6	Agencies must have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks infrastructures and applications.
26	INFOSEC 7	Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the agency operates.
27	PHYSEC 1	Agency heads must provide clear direction on physical security through the development and implementation of an agency physical security policy and an agency physical security plan.
28	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.
29	PHYSEC 3	Agencies must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.
30	PHYSEC 4	Agencies must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.
31	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.

Mandatory Requirements – summary table		
32	PHYSEC 6	Agencies must implement a level of physical security measures that minimises or removes the risk of ICT equipment and information being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
33	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: *Protective Security Policy Framework*, June 2010.

Index

Series Titles

ANAO Audit Report No.1 2010–11
Implementation of the Family Relationship Centres Initiative
Attorney-General's Department
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.2 2010–11
Conduct by Infrastructure Australia of the First National Infrastructure Audit and Development of the Infrastructure Priority List
Infrastructure Australia

ANAO Audit Report No.3 2010–11
The Establishment, Implementation and Administration of the Strategic Projects Component of the Regional and Local Community Infrastructure Program
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.4 2010–11
National Security Hotline
Australian Security Intelligence Organisation
Attorney-General's Department
Australian Federal Police

ANAO Audit Report No.5 2010–11
Practice Incentives Program
Department of Health and Ageing
Medicare Australia

ANAO Audit Report No.6 2010–11
The Tax Office's implementation of the Client Contact - Work Management - Case Management System
Australian Taxation Office

ANAO Audit Report No.7 2010–11
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2009 Compliance)

ANAO Audit Report No.8 2010–11
Multifunctional Aboriginal Children's Services (MACS) and Crèches
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.9 2010–11
Green Loans Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency

ANAO Audit Report No.10 2010–11
Centrelink Fraud Investigations

ANAO Audit Report No.11 2010–11
Direct Source Procurement

ANAO Audit Report No.12 2010–11
Home Insulation Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency
Medicare Australia

ANAO Audit Report No.13 2010–11
Implementation and Administration of the Civil Aviation Safety Authority's Safety Management System Approach for Aircraft Operators

ANAO Audit Report No.14 2010–11
Capitalisation of Software
Australian Bureau of Statistics
Civil Aviation Safety Authority
IP Australia

ANAO Audit Report No.15 2010–11
Food Standards Australia New Zealand

ANAO Audit Report No.16 2010–11
Centrelink's Role in the Process of Appeal to the Social Security Appeals Tribunal and to the Administrative Appeals Tribunal
Centrelink
Department of Education, Employment and Workplace Relations
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.17 2010–11
2009–10 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.18 2010–11
Government Business Managers in Aboriginal Communities under the Northern Territory Emergency Response
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.19 2010–11
Army Aboriginal Community Assistance Program
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.20 2010–11
Administration of the Wine Equalisation Tax
Australian Taxation Office

ANAO Audit Report No.21 2010–11
Indigenous Housing Initiatives: the Fixing Houses for Better Health program
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.22 2010–11
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2010

ANAO Audit Report No.23 2010–11
Home Ownership of Indigenous Land Program
Department of Families, Housing, Community Services and Indigenous Affairs
Indigenous Business Australia

ANAO Audit Report No.24 2010–11
The Design and Administration of the Better Regions Program
Department of Regional Australia, Regional Development and Local Government

ANAO Audit Report No.25 2010–11
Administration of the Trade Training Centres in Schools Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.26 2010–11
Management of the Tender Process for a Replacement BasicsCard
Department of Human Services

A**NAO Audit Report No.27 2010–11**
Restoring the Balance in the Murray-Darling Basin
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.28 2010–11
Management of the Australian Broadband Guarantee Program
Department of Broadband, Communications and the Digital Economy

ANAO Audit Report No.29 2010–11
Management of the Implementation of New Policy Initiatives
Australian Federal Police

ANAO Audit Report No.30 2010–11
Digital Education Revolution Program—National Secondary Schools Computer Fund
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.31 2010–11
Administration of the Superannuation Lost Members Register
Australian Taxation Office

ANAO Audit Report No.32 2010–11
Northern Territory Night Patrols
Attorney-General's Department

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office website.

Strategic and Operational Management of Assets by Public Sector Entities –	
Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	June 2010
Planning and Approving Projects	
an Executive Perspective	June 2010
Innovation in the Public Sector	
Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0	
Security and Control	June 2009
Preparation of Financial Statements by Public Sector Entities	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
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
Legal Services Arrangements in Australian Government Agencies	Aug 2006
Administration of Fringe Benefits Tax	Feb 2006

User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006