The Auditor-General
Audit Report No.18 2011–12
Performance Audit

Information and Communications Technology Security: Management of Portable Storage Devices

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81225 X

Australian National
Audit Office

Canberra ACT
20 December 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*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Information and Communications Technology Security: Management of Portable Storage Devices*.

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, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

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
Steven Favell
Bronwen Jaggers
William Na
Felicity Squires
Michael White

Contents

Tables

Figures

Abbreviations

AGD	Attorney-General's Department
AISEP	Australian Information Security Evaluation Program
ANAO	Australian National Audit Office
ATO	Australian Taxation Office
CAC Act	the *Commonwealth Authorities and Companies Act 1997*
CD/DVD	Compact Disc / Digital Versatile Disc
DSD	Defence Signals Directorate
FMA Act	the *Financial Management and Accountability Act 1997*
GB	Gigabyte
ICT	Information and Communications Technology
ISM	*Information Security Manual*
ITSA	Insolvency and Trustee Service Australia
OAIC	Office of the Australian Information Commissioner
PM&C	Department of the Prime Minister and Cabinet
PSD	Portable Storage Device
PSM	Protective Security Manual
PSPF	Protective Security Policy Framework
SOE	Standard Operating Environment
USB	Universal Serial Bus

Glossary

Cyber [space, technology, etc]	The Internet, and everything connected to it.[1]
Encryption	Encryption provides a way to distribute or receive information in secret code, so that only the intended parties can read or send it. In an ICT context, encryption is used to protect against the risk of information being intercepted, and to provide proof of the integrity and origin of the data.
Hardening	ICT system hardening is designed to minimise the security risks associated with its use. In particular, software security can degrade over time and it is important for organisations to continue to harden their Standard Operating Environment software via regular virus updating, patching and limiting the number of users with administrative privileges.
ICT	Information and Communications Technology (ICT) refers to technologies that enable information to be accessed, stored, processed, transformed, manipulated and disseminated, including the transmission or communication of voice, image and/or data over a variety of transmission media.[2]

[1] Speech by Mr Mike Burgess, DSD Deputy Director Cyber and Information Security, to the *Technology in Government and the Public Sector Summit*, August 2011, available at: <http://www.dsd.gov.au/speeches/20110808_DDCIS_TechInGovt.pdf>, [accessed 6 October 2011].

[2] Australian Bureau of Statistics, *ICT and Innovation Statistics Glossary*, last updated September 2010, available at: <http://www.abs.gov.au/websitedbs/c311215.nsf/22b99697d1e47ad8ca2568e30008e1bc/c49fb25ed58f2ec4ca25702f001eeaaa!OpenDocument>, [accessed 31 October 2011].

Internet	The Internet is the communications system created by the interconnecting networks of computers around the world.
Malware	Short for 'malicious software'. Malware attempts to subvert the confidentiality, integrity or availability of an ICT system, often by gaining administrative privileges.
Privacy	In the context of this audit 'privacy' is used with the meaning conferred by the *Privacy Act 1988* and overseen by the Office of the Australian Information Commissioner, that is: privacy related to personal information. Personal information is information that identifies or could identify a person, such as their name or address, medical records, bank account details, photos, videos—any information where the person is reasonably identifiable.[3]
Social engineering or spear phishing	Social engineering or spear phishing is a technique used by malicious attackers in which a legitimate-looking email message is sent to the target. The message may use information about the target that has been gathered from publicly available information, for example from social networking websites. The attackers may be trying to deceive people into performing actions such as opening an executable file or clicking on an internet link, thereby facilitating a malware intrusion on the computer; or disclosing personal or business-related information.[4]

[3] Office of the Australian Information Commissioner, *What is Privacy?* available at: <http://www.privacy.gov.au/aboutprivacy/what>, [accessed 24 October 2011].

[4] Defence Signals Directorate (DSD): *Detecting Socially Engineered Emails*, *Onsecure* website (login required), [accessed 2 August 2011].

Summary and Recommendations

Summary

Introduction

1. Governments, businesses, organisations and individuals use Information and Communications Technology (ICT) for a variety of purposes and functions. Government agencies rely on ICT systems to conduct their core business, and the information collected, stored and transmitted via agency ICT systems includes dealings with international governments, State and local governments, business, not-for-profit and interest groups, and individuals.

2. The protection of government information requires constant vigilance on the part of agencies because of the variety of systems and communication channels used, the increasing 'portability' of information, and the ever-present risk of cyber attack.

3. The focus of this audit is the measures taken by agencies to protect against the information security risks posed by Portable Storage Devices (PSDs). A PSD is a portable electronic device, which can be capable of storing large volumes of data (for example, a USB flash drive, CD/DVD or a portable hard drive) and/or transmitting data via voice or email and connecting to the Internet (for example, laptop computers, smartphones or tablet computers).

4. The convenience of using PSDs to store and transfer data and connect to the Internet has supported an increase in their use by agencies as part of day-to-day activities. In particular, PSDs assist agencies to engage in flexible work practices such as working away from the office, either at home or when travelling.

5. However, there are a number of risks associated with the use of PSDs, particularly due to their size and portability. The risks include the loss and/or theft of data, and the introduction of viruses and malware into the organisation's ICT environment.[5] The consequences of these risks are that government data relevant to national security, decision-making, commercial interests or the privacy of Australian citizens could be accessed by unauthorised persons. There are a number of reported instances, both in

[5] Trusted Information Sharing Network for Critical Infrastructure Program, *Portable Data Storage Security Information for CIOs/CSOs*, November 2009.

Australia and overseas, of government data being inappropriately accessed as a result of lost or stolen PSDs.

6. To address these and other security risks, the Australian Government has directed agency Chief Executive Officers (CEOs), via the Protective Security Policy Framework (PSPF), to have effective protective security programs that ensure:

- their agency's capacity to function;
- maintenance of 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.[6]

7. Included in the PSPF are a number of mandatory requirements and guidelines regarding ICT security, including for agency use of PSDs. Additionally the *Information Security Manual* (ISM) written by the Defence Signals Directorate (DSD), outlines mandatory and recommended technical controls for agency ICT systems and hardware, including PSDs.

Audit objective, criteria and scope

8. The objective of the audit was to assess the effectiveness of the management of risks arising from the use of PSDs in selected Australian Government agencies. The PSDs included within the scope of this audit were: USB flash drives; CDs and DVDs; external hard drives; laptop computers and smartphones.

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

- the Australian Taxation Office (ATO);
- the Insolvency and Trustee Service Australia (ITSA); and
- Australian Hearing.[7]

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

10. This cross-section of agencies was selected as representative of Commonwealth agencies and ICT systems, and each uses the PSDs included within the scope of this audit. Additionally, each agency collects, stores and transmits personal information relating to Australian citizens.

11. To address the audit objective, the ANAO examined the extent to which agencies had an effective framework in place for the management of PSDs, including risk assessments; policies and procedures; hardware and software controls; staff training and awareness activities; and incident response and reporting mechanisms.

12. The audit criteria and testing were based on the requirements of the PSPF and the ISM.

13. Under Government policy directions, the ATO and ITSA must meet the requirements of the PSPF and ISM. However, at the time of this audit, Australian Hearing was not required to meet these requirements as the agency had not been directed by its Minister to follow the PSPF and ISM.[8] Accordingly, the ANAO is reporting on Australian Hearing's compliance with the PSPF and ISM as a benchmark of the minimum standard required for security of Government information rather than a formal requirement.

14. The audit was conducted with the support of the Attorney-General's Department (AGD) and the specialist advice of the Office of the Australian Information Commissioner and DSD. The ANAO appreciates the assistance provided by these agencies during the course of the audit.

---

[7] Australian Hearing is an entity under the *Commonwealth Authorities and Companies Act 1997* (the CAC Act), not an agency as defined by the *Financial Management and Accountability Act 1997* (the FMA Act). However, the *Protective Security Policy Framework* and the *Information Security Manual* refer to 'agencies'. For ease of reference, this report will refer to Australian Hearing as an agency.

[8] The PSPF and ISM apply to: 'those agencies subject to the FMA Act; those subject to the CAC Act who have been directed by their Minister to follow the general policies of the government; and other bodies established for a public purpose under a law of the Commonwealth, where the body or agency has been directed by their Minister that the PSPF applies to them'. Source: <http://www.ag.gov.au/pspf>, [accessed 8 August 2011]. AGD has also advised that CAC Act entities can only be directed by their Minister to apply the PSPF if such a direction is allowable under their legislation or constitution. See also the discussion at paragraphs 1.49 to 1.53.

Overall conclusion

15. The rapidly developing world of the Internet and associated ICT systems and devices has transformed the way government operates. The significance of this transformation and the risks involved in the use of ICT systems and devices has been recognised, with a Cyber White Paper currently under development (due to be released in 2012). The White Paper's objective is to:

> …ensure Australia is well prepared to optimise the benefits of greater online engagement, and…outline how government, industry and the community can work together to address the challenges and risks arising from greater digital engagement.[9]

16. Agencies are increasingly using PSDs to assist their day-to-day operations. These devices are designed to be 'user friendly' and to facilitate quick and efficient transfer of information. While this brings great benefits, there are also ever-present risks, including the accidental loss or theft of information facilitated by the use of a PSD, and exposure of agency ICT systems to viruses and malware.

17. Central to agencies' use of PSDs, and other existing and emerging technologies, is the question of how to balance the advantages of their use with appropriate security measures to protect sensitive data.

18. Agency CEOs are responsible for ensuring that the information their organisation holds is adequately protected, and the Attorney-General's Directive makes it clear that agency heads are to ensure that protective security is a part of their agency's culture.[10] As previously reported by the ANAO, 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 assessments of the Government's security requirements, including those of the PSPF and ISM.[11]

---

[9] Department of the Prime Minister and Cabinet (PM&C), Public Discussion Paper: *Connecting With Confidence – Optimising Australia's Digital Future*, August 2011, p. 5.

[10] The Directive applies to those agencies subject to the FMA Act and certain other bodies – see footnote 8. The Hon. Robert McClelland MP, *Directive on the security of Government Business*, op.cit.

[11] ANAO Audit Report No.33 2010–11 *The Protection and Security of Electronic Information Held by Australian Government Agencies*, March 2011, p. 17.

19. There is a range of possible approaches that agencies can take in their management of PSDs, ranging from a complete 'lock down' of all connections to the ICT network, through to an accepted use of personal devices for work purposes. Against this background, agencies should assess the business need for the use of PSDs against the security risks particular to their organisation, and monitor their experience over time.

20. This audit examined the extent to which the three audited agencies had considered both the opportunities and risks presented by PSDs, and the adequacy of their risk assessments, policies and procedures, ICT security controls, training and awareness activities, and incident response procedures.

21. Overall, the audit concluded that the ATO had taken steps to effectively manage the risks associated with the use of PSDs in that agency. However, ITSA and Australian Hearing had scope to significantly improve their approach, particularly in relation to:

- risk assessments of the capacity in which PSDs may be used, and the type of information they can transmit and store;
- policies and procedures articulating the accepted parameters for the use of PSDs in the organisation;
- ICT controls for the use of PSDs being appropriate to the identified organisational risks;
- security training and awareness programs addressing the risks associated with the use of PSDs and agency expectations of their staff; and
- security incident response mechanisms covering the possible theft or loss of PSDs and processes for managing the associated risks of these incidents.

22. The report's recommendations, which are directed to ITSA and Australian Hearing improving their management of PSDs, may have broader application to other public sector agencies. The audit also highlights several areas of better practice that may be of wider benefit.

Key findings by chapter

Risk assessments (Chapter 2)

23. The PSPF aims to assist agency CEOs in taking a risk-managed approach to security in their organisations. As part of the PSPF's overarching framework, there are several mandatory requirements for agencies to undertake risk assessments and implement appropriate controls to mitigate residual risk. This applies to PSDs, which may fall both within the 'asset' and 'information' realms of protective security.

24. Additionally, better practice, as outlined by the Privacy Commissioner,[12] would see agencies use PSDs based on a risk assessment of how the devices are used, and the type of information they store.

25. While the ATO had a robust risk assessment framework in place for its use of PSDs, ITSA and Australian Hearing had not conducted specific risk assessments for the use of PSDs or adequately considered the risks associated with these devices as part of their wider agency risk management processes.

26. As risk assessments provide the vital underpinning for a layered approach to ICT security (incorporating policies and procedures, ICT controls, training and awareness activities and incident response procedures), the ANAO has recommended that agencies include in their risk management activities a risk assessment of their use of PSDs, and develop and document risk mitigation strategies where necessary.

Policies and procedures (Chapter 3)

27. Agency policies and procedures assist staff in their day-to-day business and are designed to assist with compliance, legislative and other requirements. In the protective security context, clear policies aid staff to understand their agency's security risks, and the agency's expectations of them with regard to security responsibilities. Procedures are often technical documents that set out working requirements, for example Standard Operating Procedures for ICT staff set out the required actions in a number of scenarios, including incident response.

---

[12] The Office of the Privacy Commissioner, *Public Sector Information Sheet 3 – Portable Storage Devices and personal information handling*, May 2009.

28. The PSPF and ISM require agencies to have documented policies and procedures for the management of PSDs. The Privacy Commissioner has also provided some guidance on topics for agencies to consider including in their policies and procedures for PSD use.

29. Each agency could make some improvements to their policies and procedures for the way their staff are to use PSDs, although at the ATO this was considered to be minor in nature. In line with the Privacy Commissioner's guidance, policies and procedures are expected to be based on a risk assessment and to cover key considerations such as the permitted uses of PSDs and the type of information they are permitted to hold, and expected practices for disposal and incident reporting.

30. Accordingly, the ANAO has recommended that agencies review their existing policies and procedures, or develop new policies and procedures, that clearly state the accepted parameters for PSD use. Policies and procedures for security matters in general (and relevant to this audit, PSD use), should be readily available to staff and reinforced via training and awareness programs.

Hardware and software controls (Chapter 4)

31. Appropriate ICT controls are a vital element to an effective overall approach to security for PSDs in agencies. An effective risk assessment will highlight the most appropriate controls in individual agencies to mitigate identified security risks. Agency ICT controls should also be in line with the Government's requirements set out in the ISM and other DSD publications such as hardening guides and formal evaluations of ICT equipment.

32. The ANAO tested agencies' ICT controls for PSDs against a number of ISM controls. In light of potential security concerns, the ANAO's findings have not all been reported in detail in this report. However, the findings were provided to each of the agencies during the course of the audit.

33. Overall, the ATO had implemented ICT controls that met the requirements of the ISM and adequately addressed the risks of PSDs to that organisation. However, both ITSA and Australian Hearing could improve aspects of their ICT controls framework.

34. The ANAO observed that a common weakness was in the ICT controls for the use of USB flash drives and CDs/DVDs. Due to their size, portability and capacity to store large amounts of data, these devices can pose security risks to agencies.

35. ITSA's laptop computers did not have hard disk encryption at the time of the audit, however, ITSA advised the ANAO that all of its laptops were expected to have hard disk encryption early in 2012.

36. Australian Hearing laptop computers had a number of control weaknesses at the time of the audit. Australian Hearing advised that it was working to address many of these issues, while continuing to consider the business impact of implementing other controls.

37. The ANAO has recommended that agencies implement hardware and software controls that mitigate the risks specific to their organisation.

Staff training and awareness (Chapter 5)

38. Mandatory requirements of the PSPF and ISM, and the Privacy Commissioner's better practice guidance, all recognise the importance of training and awareness programs in enabling agencies to build a security culture.

39. The ATO had a comprehensive security training and awareness program that covered the risks associated with the use of PSDs. However, ITSA and Australian Hearing could improve their approach to security training and awareness in their organisations.

40. At ITSA a comprehensive security training session had been run in previous years but this had been an ad-hoc arrangement, with no plan or framework for ongoing security training and awareness programs. While Australian Hearing was developing a formal training framework including online delivery of security training, this was not in place at the time of the audit.

41. The ANAO has recommended that the security training and awareness programs of both agencies address the risks of PSDs to their organisation.

Lost and stolen Portable Storage Devices (Chapter 6)

42. Incident response procedures are an important part of any agency's security management framework. These procedures document the steps to be undertaken in the event of a security incident (physical, personnel or information security). In an ICT security and more specifically, PSD security context, an incident response procedure should outline the expected responses both from general agency staff and the officer/s assigned responsibility for managing security incidents.

43. In each agency, policies and procedures gave clear advice to staff about their reporting obligations in the case of a lost or stolen device. However, at ITSA and Australian Hearing there were not adequately documented procedures that detailed the incident response steps required of responsible officer/s.

44. Another element that was not addressed by the two agencies was the reporting of lost or stolen devices to DSD.[13] While individual incidents may appear innocuous, DSD uses reports of these incidents to identify and respond to trends across government, and to develop new policies, procedures, techniques and training measures.[14]

45. The ANAO has recommended that agency incident response procedures include steps to respond to the theft or loss of a PSD.

Summary of agency responses

46. Agencies' general comments on the audit report are below. The responses from ITSA and Australian Hearing for each recommendation are included in the body of the report, directly following each recommendation.

Australian Taxation Office

47. The Australian Taxation Office (ATO) welcomes the audit report on *Information and Communications Technology Security: Management of Portable Storage Devices* and agrees with the Australian National Audit Office overall assessment that steps have been taken to effectively manage risks associated with the use of Portable Storage Devices (PSDs).

48. The review highlights that the ATO is compliant in all fields of Information and Communications Technology controls such as, USB flash drives, CDs/DVDs, laptop computers and smart phones. The review also identifies our robust risk assessment framework for the use of PSDs, as well as our comprehensive security training and awareness programs. We acknowledge that the five recommendations noted in the report are not directed to the ATO.

---

[13] This is a requirement of the ISM 2010 (termed 'media' in the ISM).

[14] *Information Security Manual* 2011, p. 68. Agency ICT security staff can become members of DSD's *Onsecure* website which provides advice on cyber security and an online incident reporting tool. See <http://www.onsecure.gov.au>.

49. Overall, the Tax Office appreciates the recognition given for the work we have undertaken to ensure we have highly developed practices for the management of PSDs.

Insolvency and Trustee Service Australia

50. The Insolvency and Trustee Service 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. The Insolvency and Trustee Service Australia agrees with the recommendations in the report.

Australian Hearing

51. Australian Hearing notes that while not currently subject to the requirements used to measure the organisation's management of PSDs, the audit findings do provide a valuable baseline for comparison against organisations that are subject to them. Australian Hearing welcomes the recommendations made by ANAO and effort has commenced to address the risks posed by Portable Storage Devices to the Australian Hearing environment.

Recommendations

The following recommendations apply to ITSA and Australian Hearing. However, they may also be relevant for other government 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 is addressed by practices already in place.

Recommendation No. 1
Paragraph 2.20

The ANAO recommends that agencies include in their risk management activities an assessment of their use of Portable Storage Devices, and develop and document mitigation strategies where necessary.

ITSA and Australian Hearing: *Agreed*.

Recommendation No. 2
Paragraph 3.20

The ANAO recommends that agencies review their existing security policies and procedures, or develop new policies and procedures, that clearly state the parameters for the use of Portable Storage Devices, in line with the Government's policy requirements and better practice guidelines.

ITSA and Australian Hearing: *Agreed*.

Recommendation No. 3
Paragraph 4.57

The ANAO recommends that agencies implement hardware and software controls for Portable Storage Devices that mitigate identified security risks.

ITSA and Australian Hearing: *Agreed*.

Recommendation No. 4
Paragraph 5.36

The ANAO recommends that agency security training and awareness programs address the risks of Portable Storage Devices to their organisation.

ITSA and Australian Hearing: *Agreed*.

Recommendation No. 5
Paragraph 6.35

The ANAO recommends that agency incident response procedures cover the theft and loss of Portable Storage Devices, including Defence Signals Directorate reporting requirements and the Privacy Commissioner's better practice guidelines.

ITSA and Australian Hearing: *Agreed*.

Audit Findings

1. Introduction

This chapter provides an overview of the Government's framework for Information and Communications Technology security and includes background information about the audit.

The importance and risks of Information Communications Technology

1.2 Information and Communications Technology (ICT) underpins every aspect of our modern lives. Technologies such as mobile telecommunications, the Internet, desktop and portable computers and more complex computer networks are used by governments, businesses, organisations and individuals for a variety of purposes and functions.[15]

1.3 The type of information collected, stored and transmitted via the Government's ICT systems includes dealings with international governments, State and local governments, business, not-for-profit and interest groups, and individuals. The protection of this information requires constant vigilance on the part of agencies, because of the variety of systems and communication channels used, the increasing 'portability' of information, and the ever-present risk of cyber attack.

1.4 In June 2011 the Attorney-General announced the development of a Cyber White Paper, stating that government and private sector ICT systems were under 'continuous attack' from foreign intelligence agencies, criminal organisations, and commercial competitors.[16]

Portable Storage Devices

Types of Portable Storage Device

1.5 A Portable Storage Device (PSD) is an electronic device which can be capable of storing and transferring large volumes of data. A PSD may be exclusively used for data storage (for example, a USB flash drive, CD/DVD or portable hard drive), or may also be capable of many other functions such as

[15] Attorney-General's Department (AGD), *Cyber Security Strategy*, Commonwealth of Australia, 2009, p. 1.

[16] The Hon. Robert McClelland MP, Attorney-General, *Cyber Security and launch of the Cyber White Paper*, speech during Cyber Security Awareness Week, 3 June 2011.

communication via voice or email, transmitting data, and connecting to the Internet (for example, laptop computers and smartphones).

1.6 The PSDs that are included in this audit, the volume of data they may hold, and the commercial cost, are set out in the table below.

Table 1.1

Portable Storage Devices included in this audit: background information

PSD	Amount of data capable of holding*	Cost guide*
USB flash drive (also known as thumbdrives, USB sticks) Data storage capacity only. Data transfer only via a physical connection (eg ,plugging into a computer).	Available with various capacities from 1 gigabyte (GB) to 256 GB. As a guide, an 8 GB device could hold hundreds of thousands of typed Word or Excel document pages; or – 6000 digital photos, or – 2000 mp3 songs, or – 8 feature-length movies.	$15 to $20 for an 8GB device.
CDs and DVDs which have a read/write capacity Data storage capacity only. Data transfer only via a physical connection (eg, in a computer's CD/DVD drive).	A common capacity for DVDs is 4.7 GB.	$15 for a pack of five DVDs with 4.7 GB capacity.
External hard drive Data storage capacity only. Data transfer only via a physical connection.	1 terabyte or more (1000 GB).	$90
Laptop computers Data storage and transfer capabilities including wireless communications (ie, connection to Internet and other communications).	Hard drives range from 250 GB to 1 terabyte.	$500 to $2000
Smartphones and Personal Digital Assistants (PDAs) Data storage and transfer capabilities (see above).	Up to 32 GB.	$600 to $800

Source: ANAO.

* The column describing the amount of data that may be held is a guide only, based on ANAO research in November 2011. The cost guide is based on an ANAO search of a number of online retail websites, November 2011.

Risks associated with Portable Storage Devices

1.7 The convenience of using PSDs to store and transfer data has seen them increasingly used by agencies as part of their day-to-day work. However, there are a number of risks associated with their use, particularly due to their small size and portability. The risks include[17]:

- external loss and theft—PSDs' size make them particularly susceptible to loss or theft by an unauthorised person. If the data is not encrypted it can be easily accessed;
- 'insider' data theft—PSDs provide a ready means by which data can be stolen from an ICT system, and because they are often small they can be moved in and out of a controlled environment without attracting attention. Additionally, because they are commonplace, theft of data can occur in plain sight (for example, using a CD/DVD or USB flash drive at a desktop computer is not an uncommon sight)[18];
- data loss—if data is stored only on a PSD, there is the risk of accidental or deliberate loss of the data if the device itself fails;
- introduction of viruses and malicious software ('malware')—PSDs can provide a conduit for viruses and malware to enter an ICT system, either deliberately by an attacker or unintentionally by a user;
- inadequate disposal—simply deleting data from PSDs does not completely erase it, and there are software and hardware products available that can recover deleted data which could be used by an unauthorised person; and
- introduction of unwanted software—while not posing a security risk such as viruses and malware, unwanted software such as games may affect the performance of an ICT system and corporate productivity, or introduce illicit or illegal material such as pornography or media downloaded without copyright protections.

---

17 Trusted Information Sharing Network for Critical Infrastructure Program, op.cit.

18 This was the method allegedly used by a US Department of Defense employee in downloading data later provided to Wikileaks. The documents were allegedly transferred onto a CD as the user pretended to listen to Lady Gaga music. 'How 250,000 US Embassy cables were leaked' *The Guardian*, UK, 28 November 2010, available at: <http://www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked>, [accessed 5 December 2011].

1.8 The consequences of these risks are that data relevant to national security, commercial interests or the privacy of Australian citizens could be accessed by unauthorised persons. The Attorney-General's Department (AGD) and Defence Signals Directorate (DSD) have expressed a particular concern that aggregate personal data provides opportunities for identity theft, increasingly targeted by organised crime syndicates.[19]

1.9 There are a number of documented instances of data loss and/or theft involving government-issued PSDs, both in Australia and overseas. Some are outlined in Figure 1.1 below.

[19] AGD, *National Organised Crime Response Plan Overview 2010-2013*, Commonwealth of Australia, 2010.

Figure 1.1

Examples of security incidents arising from PSDs

Australia 2011: A Defence Department contractor left a USB flash drive in the seat pocket of a commercial aircraft. The unencrypted device was handed to a radio announcer. In a statement Defence said that while the device contained a number of classified documents, none of these were 'highly classified'.[20]

Australia 2008: An Australian Federal Police (AFP) officer left a USB flash drive in a hotel computer in Kathmandu, Nepal. The USB device allegedly contained photographs of Australian victims of a plane crash, and Australian diplomatic cables. Details of some documents were given to an Australian newspaper. The AFP acknowledged the security breach.[21]

US 2008: A USB flash drive inserted in a military laptop in the Middle East contained malicious code that spread (undetected for a period) across classified and unclassified systems. The code allowed data to be transferred to servers under foreign control. The Deputy Defense Secretary stated that the code was placed on the flash drive by a foreign intelligence agency.[22]

UK 2007: Her Majesty's Revenue and Customs office lost two CDs containing the details of everyone in the UK who claimed and received child benefits. The details included names, dates of birth, national insurance numbers, and banking details. The unencrypted CDs were lost when they were sent via courier intended for the National Audit Office. Described as the 'biggest privacy disaster by our government' by the UK's Assistant Information Commissioner, it resulted in the resignation of the CEO of HM Revenue and Customs Office. The CDs were never found.[23]

Australia 2006: A senior Defence official left a CD in an airport lounge computer. The CD, containing a draft report into a sensitive matter, was found and handed to a public broadcaster.[24]

Source: Media reports, see footnotes.

[20] 'Defence investigates lost and found memory stick', *IT News*, 14 March 2011.

[21] 'AFP security breach exposed', *The Age*, 8 November 2008, and 'AFP investigates alleged security breach', *AFP Media Release*, 8 November 2008.

[22] 'Flash drive crippled Pentagon', *The Australian*, 26 August 2011.

[23] 'UK government reveals its biggest privacy disaster', *CNET*, 21 November 2007.

[24] '[Defence] report lost and leaked', *Sydney Morning Herald*, 17 May 2006.

The Government's approach to Information and Communications Technology security

1.10 There is a recognised balance to be struck between the public's right to information about government and its decisions, and the need to protect certain information from unauthorised access. Recent reforms to the *Freedom of Information Act 1982* were aimed at delivering more effective and efficient access to government information and promoting a culture of disclosure.[25] In May 2011 the Government adopted the *Principles on open public sector information*, which state the 'default position' for government information is:

> If there is no legal need to protect the information, it should be open to public access….Agencies should use information technology to disseminate public sector information, applying a presumption of openness and adopting a proactive publication stance.[26]

1.11 The *Principles on open public sector information* require open government 'if there is no legal need to protect the information'.[27] The Office of the Australian Information Commissioner (OAIC) has stated that a 'legal need' may arise for various reasons, including data security and personal and business confidentiality.[28]

1.12 Security in Australian Government agencies is governed by the Protective Security Policy Framework (PSPF). The PSPF recognises that the appropriate protection of information will be a result of agencies developing a 'security culture', stating that:

---

[25] The Hon. Anthony Byrne MP, Parliamentary Secretary to the Prime Minister, 'Second Reading Speech: Freedom of Information Amendment (Reform) Bill 2009', *House of Representatives Hansard*, 26 November 2009.

[26] Office of the Australian Information Commissioner (OAIC), 'New principles open up public sector information', Media Release 25 May 2011, available at: <http://www.oaic.gov.au/news/media_release_principles_public_sector_info.html>, [accessed 1 July 2011].

[27] OAIC, *Information Policy: Principles on open public sector information*, May 2011, available at: <http://www.oaic.gov.au/publications/agency_resources/principles_on_psi_short.pdf>, [accessed 1 July 2011].

[28] ibid., p. 12.

> …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').[29]

1.13 In December 2008 the then Prime Minister delivered the *National Security Statement*, outlining the key national security interests and challenges for Australia. The Statement identified cyber security as a key new security challenge.[30] Arising out of the *Australian Government e-Security Review 2008*[31] and complementing the *National Security Statement*, the Government's *Cyber Security Strategy* was released in 2009, outlining measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.[32]

Cyber White Paper

1.14 On 3 June 2011, the Government announced that it would develop a Cyber White Paper (the White Paper), provisionally titled *Connecting with Confidence*, to be released in the first half of 2012. The aim of the White Paper is to provide a 'comprehensive blueprint to help Australians connect to the Internet with confidence'.[33] A discussion paper released in September 2011 stated:

> Cyber intrusions against Australian information systems are serious and persistent. Australian Government agencies, in particular, must be prepared for these intrusions so they can develop adequate responses to protect the information that is entrusted to them by the Australian people and our international allies and partners.
>
> …[there is] evidence of sophisticated cyber events on government networks. The nature of the Internet makes it difficult to attribute intrusions to particular sources, but it reasonable to assume that information held on Australian

---

29 The Hon. Robert McClelland MP, *Directive on the security of Government Business*, op.cit.

30 The Hon. Kevin Rudd MP, Address by the Prime Minister of Australia: *The First National Security Statement to the Parliament*, 4 December 2008, available at: <http://pmrudd.archive.dpmc.gov.au/node/5423>, [accessed 7 July 2011].

31 AGD website: <http://www.ag.gov.au/esecurityreview>, [accessed 30 June 2011].

32 AGD, *Cyber Security Strategy*, op.cit, p. 5.

33 Senator the Hon. Stephen Conroy, Minister for Broadband, Communications and the Digital Economy, *Cyber White Paper*, Media Release 3 June 2011.

networks is attractive to intelligence services of foreign governments and criminal syndicates.[34]

1.15 The Department of the Prime Minister and Cabinet (PM&C) is heading the development of the White Paper.

Protective security in Government agencies

1.16 Protective security for Australian Government agencies[35] is governed by the PSPF, approved by the Attorney-General in June 2010. The PSPF outlines the requirements for the protection of Australian Government resources in 33 mandatory requirements. These requirements are outlined in the core security policies and governance arrangements, and are supported by more detailed guidance in a number of protocols and guidelines.[36] The policy hierarchy of the PSPF is explained in Figure 1.2 below.

[34] PM&C, Public Discussion Paper, op.cit.

[35] The PSPF applies to all FMA Act Agencies and those CAC Act entities who have been directed by their Minister to follow the PSPF. See footnote 8 and the discussion at paragraphs 1.49 to 1.53.

[36] The PSPF is being progressively implemented from June 2011 through to July 2013.

Figure 1.2

Protective Security Policy Framework: policy hierarchy

Directive on the security of Government Business

This is an overarching statement from the Attorney-General about the responsibility of agency heads to have protective security programs that will ensure: their agency's capacity to function; the public's confidence in the government and its agencies; the safeguarding of official resources and information; and the safety of those employed to carry out the functions of government and clients.

Core protective security policies and governance arrangements (mandatory)

There are three core policies, covering personnel, physical and information security. There are also governance arrangements. The three policies and the governance arrangements incorporate 33 mandatory requirements.

Security Protocols and Guidelines (control documents)

Personnel security protocol and guidelines;

Physical security management protocol and guidelines; and

Information security management protocol and guidelines.

Agency-specific policies and procedures

Agencies need to develop, or review and update, their own specific security policies, to ensure alignment with the new requirements of the PSPF.

Reporting

From August 2013, agencies will be required to report to their Minister, and copy the Attorney-General's Department and the Auditor-General, on their compliance with the PSPF's 33 mandatory requirements. Matters related to ICT technology non-compliance must be reported to DSD, and matters relating to national security non-compliance must be reported to ASIO. Heads of agencies whose people, information or assets may be affected by non-compliance must also be notified.

Source: Protective Security Policy Framework.

1.17 While the PSPF core policies and mandatory requirements were released in June 2010, there has been a transition period between the previous policy (contained in the *Protective Security Manual)* and the new PSPF. More detailed elements of the PSPF, such as protocols and guidelines, have been progressively released since September 2010 and there is a transition period for agencies to introduce the changes required. The transition period consists of two parts, an implementation period to 31 July 2012 when the new security classification system takes full effect (see below), with a further

'grandfathering' period until 31 July 2012 to allow agencies to phase out the superseded classifications and the associated control measures.[37]

PSPF: *Information Security Management Protocol*

1.18 The PSPF's *Information Security Management Protocol* and guidelines were released in July 2011. A key element of the protocol is a new security classification system for use in Australian Government agencies. The new system replaces the former dual national and non-national security classification system and aims to provide a consistent and structured approach to the protective marking of official information. The new framework reduces the number of information classifications to four (TOP SECRET, SECRET, CONFIDENTIAL and PROTECTED) and introduces five Dissemination Limiting Markers (DLMs) for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling.[38]

1.19 Agencies have a two-year period in which to phase in the new information classification framework.

The *Information Security Manual*

1.20 The *Information Security Manual* (ISM), which is produced by DSD, outlines the technical requirements for ICT systems to protect and secure agency information. The ISM is used by agencies in conjunction with the PSPF to enable the risk-managed protection of information and systems.[39]

1.21 In August 2011 DSD released the latest version of the ISM. While the technical controls in the document remain largely the same, it is accompanied by an Executive Companion aimed at senior executives, which outlines the key ICT threats for agencies and the strategies to mitigate them.

---

[37] See Attorney-General's Department: *Understanding the PSPF and Frequently Asked Questions*: <http://www.ag.gov.au/www/agd/agd.nsf/Page/Protective_Security_Policy_FrameworkPart_7_-_Understanding_the_PSPF?open&query=PSPF:%20Transition%20interpretation>; [accessed 18 August 2011].

[38] Further information is available in the *Information security management guidelines: Australian government security classification system*, 19 July 2011, available at: <http://www.ag.gov.au/pspf>, [accessed 8 August 2011].

[39] As with the PSPF, the ISM is applicable to all agencies that fall under the *Financial Management and Accountability Act 1997* (the FMA Act) and those agencies that fall under the *Commonwealth Authorities and Companies Act 1997* (the CAC Act) that have been directed by their Minister to follow the general policies of the government. See paragraph 1.50 for more detail.

1.22 DSD has also published *Strategies to Mitigate Targeted Cyber Intrusions*, which lists 35 strategies that agencies may implement to prevent targeted cyber intrusions. First published in February 2010, the updated version published in July 2011 states that if agencies had implemented the first four strategies on the list, at least 85 per cent of the attacks that it responded to in 2010 could have been prevented.[40]

Evaluated Products

1.23 From the 1980s onwards DSD evaluated security ICT products to test whether they performed as claimed by the vendor. From 1994 this process was formalised as the Australian Information Security Evaluation Program (AISEP). Under AISEP, product evaluations were outsourced to licenced evaluators, and overseen by DSD. The evaluations were based on an internationally-agreed Common Criteria for security products.

1.24 However, over the past decade the exponential increase in individual technology products resulted in a long back-log of products waiting to receive evaluation, and therefore approval for use in government ICT systems. In 2011 the AISEP program began participating in creating technology-tailored Protection Profiles based on the international Common Criteria. The Protection Profiles are documents that contain a benchmark of security requirements that a product must meet to pass evaluation. DSD states that the Protection Profiles will shorten a product's evaluation time, provide for better assurance in a product, and allow DSD to 'influence industry to build security products that meet Australian government needs'.[41]

1.25 Products that have achieved the AISEP/Protection Profile certification are published on the Evaluated Products List (EPL), which sets out which products are certified for use with which classification of information (from TOP SECRET down), for government ICT systems.

1.26 Regarding the PSDs included in this audit, at September 2011 the EPL included software for encryption of data on laptop computers, and software

[40] The top four strategies in 2011 are: 1. Patch applications; 2. Patch operating system vulnerabilities; 3. Minimise the number of users with domain or local administrative privileges; 4. Application whitelisting to help prevent malicious software and other unapproved programs from running.

DSD, *Strategies to Mitigate Targeted Cyber Intrusions*, updated July 2011, available at: <http://www.dsd.gov.au/publications/Top_35_Mitigations.pdf>, [accessed 5 August 2011].

[41] DSD, *OnSecure* website (login required), [accessed 6 October 2011].

for smartphone and tablet devices by Research in Motion (Blackberry), but no USB flash drives or external hard drives. An EPL evaluation of Apple products such as the iPhone and iPad was underway at December 2011.[42]

Legal requirements for agencies to protect privacy

1.27 In this audit, the ANAO examined agencies' management of the risks associated with PSDs, with a particular focus on the protection of personal information. Agencies have obligations under the *Privacy Act 1998* (the Privacy Act) when handling personal information. The Privacy Act contains eleven Information Privacy Principles (IPPs), which outline how an agency may collect, use, store and disclose personal information.[43] The Privacy Act provides that an agency cannot use a contract to avoid its own obligations under the IPPs by authorising a service provider to do something that the agency itself is not permitted to do.[44]

Legislative requirement

1.28 The Privacy Act adopts a principles-based, rather than prescriptive, approach to information privacy regulation. IPP 4 outlines how Australian Government agencies, Australian Capital Territory agencies and Norfolk Island agencies are expected to store and secure personal information. All agencies must comply with IPP 4.

---

[42] DSD, *OnSecure* website (login required), accessed 12 December 2011. In addition to full EPL evaluations, DSD releases 'hardening' guides for products, including the iOS platforms used in Apple products. These guides are not as comprehensive as the full evaluations and therefore can be released more quickly, based on demand from agencies for particular technologies.

[43] OAIC, available at:<http://www.privacy.gov.au/government>, accessed 13 January 2011.

[44] *Privacy Act 1998*, Section 95B.

Figure 1.3

***Privacy Act 1988*: Information Privacy Principle 4**

4. A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Source: Privacy Act 1988, Division 2 – Information Privacy Principles.

1.29 IPP 4 is based on the principle that a person whose information is held by a government agency has a right to expect that the agency will hold it securely, and will ensure that access to the information is permitted only for legitimate purposes.[45]

1.30 Under the Privacy Act, 'personal information' is defined as:

> ...information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.[46]

1.31 The OAIC has the power to audit agencies' compliance with the IPPs and to investigate complaints regarding agencies' handling of personal information. The audits and summaries of complaint cases, as well as guidance on privacy for agencies, are published on the OAIC's website.[47]

About the audit

1.32 This audit is part of a series of cross-portfolio performance audits examining government agencies' protective security arrangements. Since 1995 the ANAO has published 12 protective security audit reports.

---

[45] The Office of the Privacy Commissioner, *Plain English Guidelines to IPPs 4-7*, February 1998.

[46] *Privacy Act 1998*, section 6.

[47] OAIC, available at:<http://www.oaic.gov.au/publications/index.html>, [accessed 3 November 2011].

1.33 The objective of this audit was to assess the effectiveness of the management of risks arising from the use of PSDs in selected Australian Government agencies.

Audit criteria and scope

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

Table 1.2

Audit objective and criteria

Audit Objective: **To assess the effectiveness of the management of risks arising from the use of PSDs in selected Australian Government agencies.**	
High-level criteria	**Considerations**
Risk assessments, policies and procedures	Have agencies conducted appropriate risk assessments for the use of PSDs, in line with the Government's security requirements and better practice?
Policies and procedures	Have agencies established a policy and procedure framework for the staff use of PSDs, in line with the Government's security requirements and better practice?
Software and hardware controls	Do agencies implement hardware and software controls on the use of PSDs, in accordance with their own risk assessments, policies and procedures, and the Government's security requirements and better practice?
Staff training and awareness	Do agencies actively promote staff awareness of the risks associated with the use of PSDs, and their expected actions, via both formal security training activities and informal communication mechanisms, in line with the Government's security requirements and better practice?
Lost or stolen devices	Do agencies have adequate incident response procedures for lost or stolen PSDs, including incident reporting in line with the Government's security requirements and better practice?

Source: ANAO.

1.35 The audit did not examine other electronic devices such as digital cameras, video cameras, reel to reel tape and external DVD recorders.

Selected agencies

1.36 The following agencies were selected for review:

- the Australian Taxation Office (ATO);
- the Insolvency and Trustee Service Australia (ITSA); and
- Australian Hearing.[48]

1.37 These agencies were selected as they represent a cross-section of agencies and ICT systems, and each use the PSDs included in this audit. Each agency collects, stores and transmits personal information relating to Australian citizens. An overview of each agency's information classification system and their use of PSDs is below. More detail is in Appendix 1.

Agencies' information classification frameworks and ICT system classification

1.38 Any discussion about the adequacy of agencies' ICT security is grounded in the classification of the information that the agency holds. The PSPF (INFOSEC 3) sets out the requirement for agencies to have an information classification regime:

> 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.[49]

1.39 The ISM sets the minimum security standards that ICT systems must achieve in order to hold each level of information—from UNCLASSIFIED up to TOP SECRET.

1.40 The ISM requires agencies to have their ICT systems accredited to hold the relevant level of classified information, at least every two years. The ISM states that 'accreditation of a system ensures that either sufficient security measures have been put in place or that deficiencies in such measures have been accepted by an appropriate authority'.[50]

1.41 Each agency's information classification regime and ICT system accreditation is outlined below.

---

[48] Australian Hearing is an entity under the CAC Act, not an agency as defined by the FMA Act. However, the *Protective Security Policy Framework* and the *Information Security Manual* refer to 'agencies'. For ease of reference, this report will refer to Australian Hearing as an agency.

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

[50] DSD *Information Security Manual* 2010, Commonwealth of Australia, p. 48.

Australian Taxation Office

1.42 The ATO had an information classification regime in place (as required by the PSPF), which was supported by policies and procedures outlining staff responsibilities for information classification and handling.

1.43 The majority of the ATO network has been certified under ISM requirements to operate at the PROTECTED level. There are several enclaves of the network that operate at a higher classification, including the area which conducts testing on the ATO's ICT security measures.

Insolvency and Trustee Service Australia

1.44 There was no formal information classification regime in force during the audit period, nor was the ITSA network accredited to ISM standards.

1.45 In November 2011, ITSA advised the ANAO that its records manager was working to provide information to ITSA management on the classification of ITSA's data, in consultation with business areas. ITSA was also seeking to appoint an external consultant to advise on the work required to classify its network to a level commensurate with the level of the data stored on ITSA equipment. The work on the ITSA network would commence in 2012.

Australian Hearing

1.46 Australian Hearing advised that it did not have a formal information classification regime in force during the audit period, nor was its ICT network accredited to ISM standards. However, as outlined below in paragraphs 1.49 to 1.53, Australian Hearing is not currently required to adhere to the Government's requirements for information classification and ICT system certification.

PSDs in use at each agency

1.47 Each agency uses the PSDs included in this audit, including for the storage and/or transmission of personal information about their clients. This use is outlined below.

Table 1.3

Audited agencies' use of Portable Storage Devices

	ATO	ITSA	Australian Hearing
USB flash drives	Around 2 500 at the ATO. Use of the USB flash drives is restricted to a specific brand of biometric USB flash drive. Staff must apply to be issued with one of these devices.	An undetermined number are in use. There is a mix of corporately-issued encrypted devices and privately-purchased non-encrypted devices.	An undetermined number are in use, primarily by corporate/support staff, with some containing marketing material provided by external sources.
CDs/DVDs	While all ATO staff may copy files[51] from a CD/DVD drive onto the ATO network, only around 200 are granted 'write' access to the drives.	An undetermined number are in use.	An undetermined number are in use, primarily by corporate/support staff, including some which contain marketing material provided by external sources.
External hard drives	A small number of external hard drives are used predominantly by technical support staff.	A small number are used primarily by technical support staff.	A small number used primarily by technical support staff.
Laptop computers	ROAM laptops[52] are issued to staff who require them for an established business need. At June 2011, approximately 3 600 staff had access to a laptop.[53]	Around 90 laptops are used by staff to work away from the office, either during fieldwork such as conducting interviews with clients or insolvency providers, at home or for travel.	450 (approx) used primarily by clinicians to perform hearing testing, fit hearing aids, and other customer service activities.
Tablet computers	Not in use at the time of the audit.	Not in use at the time of the audit.	Under consideration for use by National Board members. Would not connect to the AH network.

[51] The types of files that may be copied to and from CDs/DVDs (and other devices such as USB flash drives) is restricted by the ATO—for example, executable files may not be copied onto the ATO network.

[52] Short for Roving Office ATO Mobility.

[53] There was a smaller number of actual devices (around 3 160), as in some areas the laptops are 'pooled'—that is, shared amongst a number of staff.

	ATO	ITSA	Australian Hearing
Smartphones	In 2011 the ATO launched a trial of Blackberry smartphones, with around 200 devices issued, mainly to Senior Executive Service staff.	13 Blackberry smartphones have been issued to management staff.	Around 48 are issued mainly to management staff (mostly Apple iPhones). Staff may also seek permission to use personal smartphones phones to connect to the email network.

Source: ANAO, based on advice from audited agencies. Note this table reflects the use of PSDs at the agencies during the period of audit fieldwork, April to June 2011.

Audit approach

1.48 The ANAO gathered evidence for the audit by:

- reviewing each agency's ICT security risk assessments, policies and procedures relating to PSDs, to assess whether they established appropriate controls for the use of PSDs. This included a review of the agency's compliance with the Government's minimum standards for management of PSDs (the PSPF 33 mandatory requirements and the relevant 'must' and 'should' statements in the ISM 2010);
- interviewing agency staff to understand how PSDs are used in the agency, how PSD policies and procedures are developed and implemented, how the agency's ICT systems support the use of PSDs, and how hardware and software controls over PSDs are managed and configured;
- conducting an online survey[54] of selected agency staff to gauge how PSDs were being used in each agency, staff understanding of their agency's policies and procedures for use of PSDs, and the effectiveness of training. Details of the sampling methodology and survey approach are set out in Appendix 2; and

[54] The online survey was conducted with the assistance of ORIMA research, over a two week period at the beginning of August 2011.

- testing ICT security controls around the use of PSDs, to confirm that controls and practices reflected the agency's policies and procedures and were in line with PSPF and ISM requirements.[55]

Applicability of PSPF and ISM requirements

1.49 As outlined above, one of the criteria used by the ANAO was to examine whether agencies had complied with the mandatory security requirements detailed in the PSPF and ISM.

1.50 The PSPF and ISM are applicable to all agencies governed by the FMA Act, and entities governed by the CAC Act where their Minister has directed them to follow the 'general policies of the Australian government'.[56] The CAC Act also allows the Finance Minister to issue a General Policy Order that applies to all or some CAC Act entities (after consultation with the relevant ministers).[57] However a General Policy Order regarding the PSPF or ISM has not been issued (at the time of this audit).

1.51 Australian Hearing is a CAC Act entity and therefore the PSPF and ISM would only apply on direction from its Minister. Australian Hearing advised the ANAO that it has not received such a direction from its Minister.

1.52 The Attorney-General has emphasised the importance of 'actively managing the security risks associated with electronic data transmission, aggregation and storage'.[58] In this context, the PSPF and ISM represent a minimum standard for the management of the risks associated with the use of PSDs. Accordingly in this audit the ANAO is reporting on Australian Hearing's compliance with the PSPF and ISM as a benchmark, while noting that there is currently no official requirement for Australian Hearing to comply.

1.53 AGD advised the ANAO that at present, it has not been advised by Ministers, and does not keep a record of which CAC Act entities are subject to

---

55 As the main fieldwork period was from April to June 2011 this audit has assessed agencies' compliance with the ISM 2010, which was in force during the fieldwork period. Most of the controls remain the same in the ISM 2011.

56 *Protective Security Policy Framework*, op.cit, p. 8. AGD has also advised that CAC Act entities can only be directed by their Minister to apply the PSPF if such a direction is allowable under their legislation or constitution.

57 Section 48A of the CAC Act.

58 The Hon. Robert McClelland MP, *Directive on the security of Government Business*, op.cit.

the PSPF. As raised in previous audit reports,[59] the ANAO suggests that AGD clarify which CAC Act entities are currently subject to the PSPF and ISM and communicate this to all affected entities.

Consultation with stakeholders

1.54 The ANAO consulted with key stakeholders including the AGD, as the key policy agency for Australian government protective security arrangements; the DSD, which is the government's specialist information security agency; and the OAIC (incorporating the Privacy Commissioner), which has a specific interest in agencies' measures to protect Australian citizens' privacy, and has developed useful guidance on agencies' use of PSDs.[60] The ANAO appreciates the advice and expertise provided by staff in each of the above agencies during the conduct of the audit.

Auditing standards and cost

1.55 The audit was conducted in accordance with the ANAO's auditing standards, at a cost of approximately $386 000.

[59] ANAO Audit Report No.25 2009–10 *Security Awareness and Training*; and ANAO Audit Report No.44 2008–09 *Security Risk Management*. Available at: <http://www.anao.gov.au/Publications/Audit-Reports>, [accessed 18 October 2011].

[60] The Office of the Privacy Commissioner, *Public Sector Information Sheet 3 – Portable Storage Devices and personal information handling*, May 2009.

2. Risk Assessments

This chapter examines the audited agencies' risk assessments for the management of PSDs.

The role of risk assessments

2.1 A risk assessment is the systematic use of available information, based on the evaluation of likelihood and consequence, to determine risk.[61] In a protective security context, a key element for agencies in developing an effective protective security culture is the identification and management of security-related risks.[62]

2.2 The PSPF is designed to help agencies identify their individual levels of security risk tolerance. There are a number of mandatory requirements in the PSPF and ISM for agencies to conduct regular security risk assessments. These are outlined below.

Figure 2.1

Protective Security Policy Framework and *Information Security Manual*: Risk Management

PSPF GOV 4 – MANDATORY

Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised every two years or sooner when changes in risks and the agency's operating environment dictate.

PSPF GOV 6 – MANDATORY

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 ISO3 1000:2009 and the Australian Standards HB 167:2006 Security risk management.

PSPF INFOSEC 5 – MANDATORY

Agencies are to ensure they…conduct risk assessments and define policies and processes for mobile technologies and teleworking facilities.[63]

---

61 ANAO Audit Report No. 38 2010–11 *Management of the Certificate of Compliance Process in FMA Act Agencies*, Commonwealth of Australia, p. 8.

62 ANAO Audit Report No.44 2008-09 *Security Risk Management*, Commonwealth of Australia, p. 13.

63 Detailed requirement under INFOSEC 5: Information Access Controls.

ISM Control: 0040 – MUST
Agencies must ensure that every system is covered by a Security Risk Management Plan.

Source: *Protective Security Policy Framework*, and the *Information Security Manual 2010*.

2.3 Further, in 2009 the Privacy Commissioner[64] released detailed guidance regarding management and use of PSDs: *Public Sector Information Sheet 3: Portable Storage Devices and personal information handling* (The Privacy Commissioner's guidance).[65] The guidance outlines the importance of conducting risk assessments for PSDs, stating that they have three main purposes:

- to identify the risks of using PSDs across an agency's different activities or operations;
- to evaluate the likelihood and consequences of the risks occurring; and
- to put in place safeguards (often referred to as risk treatments) to manage the risks.[66]

2.4 The Privacy Commissioner's guidance on the key factors to consider when developing a risk assessment for PSDs is outlined below. While the guidance is focused on protecting *personal* information stored or transmitted by PSDs, the principles may also apply to other information held by agencies.[67]

[64] On 1 November 2010 the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner (OAIC). The statutory role of Privacy Commissioner is now one of the functions covered by the OAIC (see the *Australian Information Commissioner Act 2010*).

[65] The Office of the Privacy Commissioner, *Public Sector Information Sheet 3 – Portable Storage Devices and personal information handling*.

[66] ibid.

[67] It is important to note that unlike the PSPF's mandatory requirements, the Privacy Commissioner's information is guidance only.

Figure 2.2

Privacy Commissioner: Risk assessment for use of PSDs

Key factors to be considered in assessing the risks associated with the use of PSDs:

- What kind of personal information is usually stored or handled on the PSD?
- Who is likely to be affected by a security breach, where personal information is compromised?
- What types of PSDs are used to handle personal information in the agency?
- How often are PSDs used in the agency?
- Does the agency prohibit staff from using privately owned PSDs at work?
- What software and hardware controls does the agency apply to PSDs?
- How effective are current PSD controls?
- Can the agency track PSD use?

Source: Office of the Privacy Commissioner, *Public Sector Information Sheet 3 – Portable Storage Devices and personal information handling*, May 2009.

Agencies' risk assessments for Portable Storage Devices

Methodology

2.5 The ANAO reviewed each agency's risk management framework and the specific risk documentation around the use of PSDs in their organisation, where available. The ANAO was expecting to see that agencies had undertaken appropriate risk assessments, in alignment with the requirements of the PSPF and ISM, and the Privacy Commissioner's guidance (outlined in the Figures above).

Australian Taxation Office

2.6 Overall, the ANAO assessed that the ATO had implemented a robust framework for the management of risks, including those associated with the use of PSDs.[68]

[68] At the time of fieldwork, the ATO was transitioning to a new risk management framework. The ANAO's assessment is based on the risk framework that was in place during the fieldwork period (April – June 2011). However, the ANAO has reviewed documents for the new risk management framework and is satisfied that the key elements observed during the audit will continue or be enhanced in the new framework.

2.7 The ATO identified risk categories and assigned risk ratings based on detailed assessments. These assessments were conducted with consideration of the ATO's specific circumstances and environment.

2.8 The existence and effectiveness of current controls was considered, as well as the need to design new controls where the risk level remained insufficiently mitigated. Risk documents were updated regularly, in line with improvements in controls and the changing risk environment. The risk assessments also demonstrated the ATO's awareness of the need for continuous research into new and evolving vulnerabilities and methods of attacks.

2.9 Many of the treatments identified in risk management plans had been implemented. Where risks were identified, the mitigating controls applied by the ATO were consistent. These included:

- restrictions on wireless device usage;
- updating policies and procedures on use of PSDs;
- encryption and protection of information stored on PSDs;
- logging and monitoring of data transferred to and from PSDs; and
- implementing staff awareness activities.

2.10 In addition to the high-level risk activities outlined above, the ATO had a process for undertaking detailed technical assessments of hardware and software technology used within the organisation. The ATO's rationale for conducting these technical assessments was that:

> The Tax Office need not shy away from technology that can improve the functionality it provides to clients or enhance its security capability. However a formal, rigorous assessment of new devices, protocols, software and other technology must be established to ensure its risk profile is not significantly increased, that it is proven from the perspectives of both functionality and security, and that they can be introduced to the Tax Office's electronic environments with a minimum of disruption.[69]

[69] ATO, information provided to the ANAO.

2.11 The technical assessments for PSDs used by ATO included specific risk assessments of key control software, penetration tests[70] of ROAM laptops and BlackBerry smartphones, and security assessments of various brands of USB flash drives prior to vendor selection.

2.12 In some cases, the technical assessments for PSDs identified some residual risks associated with a particular device or its implementation in the ATO ICT environment. However, completing these assessments enables management to make well-informed and documented decisions that the level of risk is tolerable and accepted.

Insolvency and Trustee Service Australia

2.13 ITSA had a Risk Management Plan, finalised in 2010, which outlined a process for identifying agency risks, determining the existence of controls, assessing risks against criteria, maintaining a risk register and management review. However, the risk register detailed only one high-level risk relevant to the security of ITSA's information and systems. There was no evidence of a lower-level consideration of the risks associated with ITSA's use of PSDs.

2.14 The ANAO considers that ITSA's risk management activities at the time of the audit had not addressed the emerging ICT risks in a sufficiently detailed or timely manner. Given the fast-evolving nature of IT security and related threats, including the growth in use of and changing risk profile of PSDs, a more comprehensive assessment of protective security risks would be expected, at the very least within the two-year timeframe mandated by the GOV 4 requirement of the PSPF.

2.15 ITSA advised the ANAO that the current (November 2011) review of its IT Security Policy includes a consideration of the risks associated with the use of PSDs, and outlines mitigation strategies to reduce these risks.

Australian Hearing

2.16 Australian Hearing had a high level Strategic Risk Assessment, developed in 2010 and updated in 2011. While the Strategic Risk Assessment identified the risk of 'leakage of patient confidential data', there was no

[70] A penetration test is a program of systematic testing that identifies weaknesses inherent in ICT systems. System owners and security administrators use the results of the testing to improve the security posture of the application/system and therefore improve the security of the overall ICT environment.

detailed consideration of the risks posed by the agency's use of PSDs, in this document or in other supporting documentation. Other key documents such as an agency-wide Security Plan and an ICT system Security Risk Management Plan were not in place.[71]

2.17 Australian Hearing subsequently advised the ANAO that it has initiated a process to develop and implement an agency-wide security risk management framework, including an assessment of its use of PSDs.

Conclusion

2.18 The PSPF and ISM place an emphasis on agencies taking a risk-based approach to protective security. In addition, better practice as outlined by the Privacy Commissioner would see agencies use PSDs based on a risk assessment of how the devices are used, and the type of information they store.

2.19 While the ATO had a robust risk assessment framework in place for PSDs, including assessments of individual devices, ITSA and Australian Hearing had not conducted specific risk assessments for the use of PSDs, or adequately considered the risks associated with these devices as part of their wider agency risk assessment processes. Risk assessments should address key questions such as those outlined in Figure 2.2 above.

Recommendation No.1

2.20 The ANAO recommends that agencies include in their risk management activities an assessment of their use of Portable Storage Devices, and develop and document mitigation strategies where necessary.

ITSA response

2.21 Agreed. ITSA's Fraud Risk Assessment Plan has been updated to include the risks associated with PSDs and a management plan to address the risks. ITSA is updating its ICT Security Policy to specifically include appropriate practices for PSDs.

[71] These are requirements under the PSPF and ISM. As noted previously, while Australian Hearing is not currently required to meet these requirements, they represent better practice.

Australian Hearing response

2.22 Australian Hearing accepts Recommendation 1 and has already undertaken a process to perform an assessment of security risks across primary IT streams. This risk assessment will be expanded to include an assessment of risks identified for PSDs. This risk assessment is scheduled for completion by end of Q4 2011/12.

3. Policies and Procedures

This chapter examines each audited agency's policies and procedures for the use of Portable Storage Devices.

The role of policies and procedures

3.1 Government agencies have internal policies and procedures that assist staff in their day-to-day business and ensure compliance with legislative requirements. Clear protective security policies will assist staff to understand their agency's security risks, and the agency's expectations of them with regard to security responsibilities. Procedures are often more technical documents that set out working requirements, for example Standard Operating Procedures for ICT staff set out the required actions in a number of various scenarios.

3.2 A policy that sets out how staff may use PSDs at work can assist to address some of the risks that have been identified in the risk assessment, as discussed in Chapter 2.[72]

3.3 The PSPF and ISM both require agencies to develop security policies and procedures that meet their specific business needs. In addition, the Privacy Commissioner has provided some guidance on matters to be considered for inclusion in policies about PSD use. These are outlined in the Figures below.

Figure 3.1

Protective Security Policy Framework and *Information Security Manual*: Policies and Procedures

PSPF GOV 5 – MANDATORY

Agencies must develop their own set of protective security policies and procedures to meet their specific business need.

PSPF INFOSEC 4 – MANDATORY

Agencies must document and implement operational procedures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security.

[72] The Office of the Privacy Commissioner, *Public Sector Information Sheet 3 – Portable Storage Devices and personal information handling*.

ISM 2010 Control: 1082 – MUST (UNCLASSIFIED and above)
Agencies must develop a policy governing the use of mobile devices.

Source: Protective Security Policy Framework and *Information Security Manual 2010*.

3.4 More specific advice about matters for agencies to consider when developing a PSD policy is contained in the Privacy Commissioner's guidance, as summarised below.

Figure 3.2

Privacy Commissioner: Key factors to consider when developing a policy for use of PSDs

These factors are not in order of importance, nor are they exhaustive. Agencies should consider all the factors together before deciding what their policy needs to cover to address their own particular risks:

- Application – applies to all staff members including, where applicable, contractors, interns, consultants, etc.
- Flexibility – covers all types of PSDs used in the agency (and possibly new technologies not yet used).
- Use of PSDs to handle personal information – outlining how personal information is to be handled on PSDs, including transfer and deletion requirements.
- Privately owned PSDs – outlining whether staff may use privately owned PSDs in the workplace to handle work information, and if so, parameters around their use.
- Personal use – outlining if, and in what circumstances, agency-issued PSDs may be used for personal use.
- Sharing PSDs – outlining whether and in what circumstances staff may share PSDs externally or with other staff members.
- Personal responsibility – outlining the personal responsibilities of staff in safeguarding agency-issued PSDs.
- Obsolete or damaged PSDs – outlining the disposal process for used or damaged PSDs.
- Lost or stolen PSDs – outlining procedures for reporting lost or stolen PSDs; and
- Breach – outlining the sanctions applicable if staff breach the PSD policy.

Source: Office of the Privacy Commissioner, *Public Sector Information Sheet 3 – Portable storage devices and personal information handling*, May 2009.

Agencies' policies and procedures for Portable Storage Devices

Methodology

3.5 The ANAO reviewed each agency's policies and procedures, including evidence regarding their development (where available), and interviewed a range of agency staff. Additionally, the online survey deployed to selected staff in each agency included questions to gauge staff understanding of their agencies' policies and procedures for PSD use (see paragraph 1.48 and Appendix 2 for more detail).

3.6 Agencies were expected to have developed policies and procedures for the use of PSDs that clearly outlined the parameters for the use of PSDs, in line with the requirements of the PSPF and ISM, with regard to the Privacy Commissioner's better practice (outlined in the Figures above).

Australian Taxation Office

3.7 Overall, the ATO's policies and procedures relating to PSDs met the PSPF and ISM requirements, and the key elements of better practice as outlined by the Privacy Commissioner.

3.8 The ATO's internal policy is organised into a tiered framework which includes Corporate Practice Management Statements (CPMS—the high-level formal policies of the organisation); Corporate Management Procedures and Instructions (which provide practical guidance about how the CPMS are to be followed); and Practice Notes and Practice Statements (additional reference points which provide detail at the business line or operational level).

3.9 At the time of audit fieldwork, some of the ATO's security policies and procedures did not adhere to this tiered framework (that is, they had different titles and layouts that did not reflect the ATO's standard approach). However, a project to realign these policies and procedures, due for completion by the end of 2012, should assist ATO staff to locate the relevant documents and understand their context within the broader ATO requirements for security of information and assets.

3.10 The ANAO also observed that several of the policies and procedures outlined a mix of user and administrator responsibilities. To assist ATO staff, it may be helpful to separate these policies and procedures into 'normal business user' security policies and procedures, and IT administrator Standard

Operating Procedures (or similar). This observation was reflected in a number of free-text responses to the ANAO's online survey of ATO staff, for example:

> [it] would be beneficial if there was a summary in point form for each type of device with links to other more detailed resources that was easy to find; and
>
> There are a lot of practice statements about information security and often it is very difficult to find the answer to simple questions like 'What is the maximum information level classification type material that can be stored on your laptop'. I know the answer, but finding it in the practice statements is difficult.

3.11 The ATO agreed with the ANAO's suggestions for improvement and stated that the policy review should resolve the alignment issues and refinement of policies and procedures.

Insolvency and Trustee Service Australia

3.12 During 2011 ITSA initiated a review of all of its ICT polices and procedures. However, as the review was not complete, the ANAO's assessment was based on the policies that were in existence during the fieldwork period (April–June 2011).

3.13 Overall, ITSA's policies and procedures had insufficient detail and procedural guidance to effectively meet PSPF and ISM requirements and the Privacy Commissioner's guidance. The existing policies and procedures were at least five years old, and lacked sufficient practical information about the use of PSDs, including the acceptable and appropriate classification and storage of information on either ITSA's network or PSDs. Responses from ITSA staff in the ANAO's online survey also indicated a need for updated policies, for example:

> We use USBs currently without a policy…we need one. The normal practice is to email information around however large documents can not be sent this way. Users do not have access to shared locations across all sites and business lines so USBs have become the norm.

3.14 The ANAO acknowledges that ITSA is developing new security policies and procedures, which should address the limitations identified in this audit. To address the PSPF and ISM requirements and the Privacy Commissioner's guidance, the updated policies and procedures should address the emerging risks associated with the use of PSDs, specifically in the context of the ITSA security environment.

Australian Hearing

3.15 The policies and procedures reviewed by the ANAO generally covered the PSPF and ISM requirements and the Privacy Commissioner's guidance. A number of policies and procedures had recently been developed by Australian Hearing, however as noted previously they did not appear to have been based on a sufficiently robust risk assessment. The policies and procedures should be reviewed once a risk assessment has been conducted (see Recommendation 1).

3.16 Free-text responses to the ANAO's online survey of Australian Hearing staff indicated that staff were aware of the policy requirements for the use of PSDs:

> My agency is very particular about email/internet policy and the correct usage of items such as laptops, next G, mobile phones, DVD's etc. Policy is regularly revisited by the agency.

Conclusion

3.17 Each agency could make some improvements to their policies and procedures for the use of PSDs (although for the ATO these were minor in nature). In line with the Privacy Commissioner's guidance, policies and procedures should be based on a risk assessment, and in developing policies and procedures agencies should consider the matters highlighted in Figure 3.2 above.

3.18 Additionally, agency staff can only follow policies and procedures if they are aware of them. Agencies' policies and procedures for security matters in general (and relevant to this audit, PSD use), need to be readily available to staff and reinforced via training and awareness programs (discussed in Chapter 5).

3.19 Agencies could also look at innovative ways to promulgate their policies and procedures. For example, for Apple devices such as iPhones and iPads, DSD has suggested that agencies install policies directly on the device (in the form of a web clip), making them highly accessible to the user.[73]

[73] DSD, *iOS Hardening Configuration Guide for iPod touch, iPhone and iPad iOS 4 devices*, June 2011, p. 33.

Recommendation No.2

3.20 The ANAO recommends that agencies review their existing security policies and procedures, or develop new policies and procedures, that clearly state the parameters for the use of Portable Storage Devices, in line with the Government's policy requirements and better practice guidelines.

ITSA response

3.21 Agreed. ITSA is updating its ICT Security Policy to include parameters for the use of PSDs and other evolving technologies. This is in line with the Government's policy requirements and better practice guidelines. This document is in final draft. ITSA will continue to review ICT security documentation and processes and ensure they reflect current Government policies regarding protective security and information classification.

Australian Hearing response

3.22 Australian Hearing accepts Recommendation 2 and plans to review the Protective Security Policy Framework as published by the Attorney-General's Department with the intent to adopt the standards as appropriate to our agency. Appropriate policies and procedures will be developed around the use of PSDs based on the output of the established risk assessment by Q1 2012/13.

Figure 3.3

Better Practice Example: Policy for PSD use

ATO: National IT Security Procedure: Use of encrypted USB devices

- states the scope of who the policy applies to;
- outlines procedural steps such as how to order a device, manager approval requirements;
- gives a general overview of the accepted use of USB devices;
- gives further detail under subtitle 'Employee Responsibilities';
- clearly states the level of classified information that is permitted to be transferred to and from the device, including how the device should be used on home computers;
- outlines responsibility for shared devices;
- outlines what staff should do if a device is lost or stolen (including hotline phone number), corrupted or no longer needed for work purposes; and
- provides links to other related policies and guidelines.

The policy has been reviewed within the last two years and is accessible on the ATO intranet site.

Source: ATO, material provided to the ANAO.

4. Hardware and Software Controls

This chapter assesses the Information and Communications Technology controls for Portable Storage Devices in the three audited agencies.

The role of controls in the use of Portable Storage Devices

4.1 The use of ICT security settings, referred to as controls, is a vital element in a 'layered' approach to ICT security in government agencies.[74] As outlined in Chapter 1, the ISM outlines the technical controls that agencies are expected to implement to ensure the integrity, availability and accessibility of their information. In addition, DSD produces other guidance such as its *Strategies to Mitigate Targeted Cyber Intrusions*, hardening guides and formal evaluations for specific products, and position papers on emerging issues such as cloud computing.[75]

4.2 DSD is moving towards an enabling approach for ICT controls, particularly in relation to new and mobile technologies, as signalled by its Deputy Director in August 2011:

> DSD can't be in the business of telling people that they can't take advantage of new technology… What we can do, though, is enable them to use it in the least risky ways.
>
> This is why DSD revised the ISM's restrictions on user-owned devices connecting to government networks. Now, you can use your own devices – including your iPads – to connect into networks to read your email and browse your intranet remotely, as long as you use a trusted operating system.[76]

[74] As reflected in this report, a layered approach to ICT security will include risk assessments, policies and procedures, ICT controls, training and awareness activities, and incident response procedures.

[75] See DSD internet site: <http://www.dsd.gov.au/aboutdsd/publications.htm>, [accessed 7 October 2011].

[76] Speech by Mr Mike Burgess to the *Technology in Government and the Public Sector Summit*, August 2011, op.cit.

Agencies' hardware and software controls for Portable Storage Devices

Methodology

4.3 In each agency, the ANAO reviewed the hardware and software controls in place for each of the PSDs included in this audit (see Table 1.3), to gain a level of assurance regarding the protection of information that may be held on such devices.

4.4 In addition to the controls testing, the ANAO interviewed ICT management and help desk staff, and reviewed relevant documents such as Standard Operating Procedures, manuals, software and product risk assessments, and penetration test results. The ANAO did not conduct penetration tests on agency ICT networks.

4.5 The testing criteria were based on relevant ISM 2010 controls. The test results detailed in this chapter are not necessarily indicative of each agency's overall compliance or non-compliance with the listed ISM control. They are the ANAO's assessment of the adequacy of each agency's actions in implementing controls for the specific PSD being discussed.

4.6 In light of potential security concerns, the ANAO's findings have not all been reported in detail in this report. However, the findings were provided to each of the agencies during the course of the audit.

4.7 The criteria listed in the tables below have been adapted from the ISM 2010 to best reflect the ANAO's tests and focus on particular elements of the agencies' management of PSDs. The compliance requirements (must/should/recommended) that have been used are applicable for ICT systems and information at the UNCLASSIFIED level, unless otherwise noted.

Applicability

4.8 The ANAO notes that Australian Hearing is not currently required to implement the ISM controls framework. However, as discussed in paragraphs 1.49 to 1.53, the PSPF and ISM represent a minimum standard for security management of the risks associated with the use of PSDs. Accordingly in this audit the ANAO is reporting on Australian Hearing's compliance with the PSPF and ISM as a benchmark.

Test results for USB flash drives and CDs/DVDs

4.9 The ANAO tested agencies' compliance with a number of ISM controls for the use of USB flash drives[77] and CDs/DVDs (termed 'removable media' in the ISM). The results are set out in Table 4.1 below.

Table 4.1

ICT controls on USB flash drives and CDs/DVDs: ANAO testing

Criterion	ATO	ITSA	Australian Hearing
Mobile device storage encryption – ISM Control: 0869 (IC) Agencies should encrypt information on all mobile devices using at least a DSD Approved Cryptographic Algorithm.	✓	×	×
Connecting media to systems – ISM Control: 0342 Agencies must prevent unauthorised media from connecting to their system.	✓	⊘	×
Using media with systems – ISM Control: 0337 Agencies must not use media with a system that has a lower classification than the media.	✓	×	N/A
Registering media – ISM Control: 0946 It is recommended agencies register all media with a unique identifier in an appropriate register.	✓	×	×

Source: ANAO testing.

Legend: ✓ indicates that the control measures adequately addressed identified risks.

⊘ indicates that the control measures partially addressed identified risks.

× indicates that the control measures did not adequately address identified risks.

(IC): IN-CONFIDENCE information and system applicability.

Analysis – USB flash drives and CDs/DVDs

Australian Taxation Office

4.10 Overall, the ATO had taken steps to implement effective controls in restricting the unauthorised transfer of information, and reducing the risk of data loss via the use of USB flash drives and CDs/DVDs.

4.11 The ATO limits the number of staff who can use PSDs to store and/or transmit information outside of its secure network via the use of access

[77] This analysis also applies to portable external hard drives which have, for all intents and purposes, the same functionality as USB flash drives but with a larger data storage capacity.

controls and by limiting the types of approved devices. As at October 2010, an ATO risk assessment stated that only 220 (less than one per cent of ATO staff) had 'write' user privileges to copy data from the network onto CD/DVDs.

4.12 The ATO had restricted the use of USB flash drives to a particular brand of device. Approximately 2 500 had been issued by ATO to staff at the time of the audit. These devices are encrypted, require fingerprint authentication, and are issued following a documented approval process.

4.13 However, the ATO acknowledged that certain unauthorised devices could still be connected to the system. The ANAO acknowledges the difficulty in mitigating all potential vulnerabilities, and that the ATO's file transfer monitoring system (discussed further in Chapter 6) could assist to identify which user was logged in at the time of any unauthorised data transfer. However the vulnerability did not appear to have been identified in ATO risk assessments or have been formally reviewed by management.

4.14 As with any agency-issued or personal device, the ATO's USB flash drives also had vulnerabilities when used by staff in a non-ATO machine (for example, a home computer). Once authenticated, there is an increased risk to the data on the USB flash drive from any malicious software that exists on the non-ATO machine.

4.15 The ANAO notes that this vulnerability was identified as part of the ATO's technical assessment of USB devices.[78] To reduce the risk, ATO policies inform staff that any file classified at IN-CONFIDENCE or PROTECTED must only be accessed from the encrypted USB flash drive, and not copied to the local machine.[79] The ATO also encouraged the use of ROAM laptops where staff are routinely working on classified information outside of the office.

Insolvency and Trustee Service Australia

4.16 At the time of audit fieldwork the ANAO considered there to be a number of weaknesses in ITSA's management of USB flash drives and CDs/DVDs.

[78] See paragraphs 2.11 and 2.12.

[79] While this further reduces the risk, there is still the potential for traces of information accessed from and saved directly to a USB flash drive to remain on the non-ATO machine.

4.17 The ANAO identified two sets of practices in the management of USB flash drives, including the oversight and security of devices. ITSA's Canberra-based IT section had a process of issuing password protected, encrypted USB flash drives to staff requiring regular access to these devices. This process involved users signing an agreement form acknowledging receipt of the device and accepting the terms and conditions associated with their use.[80]

4.18 However, the ANAO observed that there was also a significant number of devices issued in a decentralised process, and no controls preventing staff from using personal devices. Site support teams at other ITSA offices had their own practices for the management of USB flash drives. These involved purchasing off-the-shelf products without security specifications such as encryption. These devices were not given asset numbers and thus not accounted for during standard stock-take procedures.[81]

4.19 This means that ITSA did not have a complete register of its corporately-issued USB flash drives, reducing management oversight, and many of the devices being used were not encrypted, password protected, or labelled. If one were to be lost or stolen, any information held on the device would be easily accessible.

4.20 Additionally, ITSA had no mechanism for tracking the transfer of files taken from, or moved onto its network. Logging of this kind provides management with a view of how staff are using the devices, and also serves to discourage and detect inappropriate behaviour (see Chapter 6).

4.21 While ITSA's SOE at the time of fieldwork included anti-virus protection and prevented normal users from installing unauthorised software, the use of unknown and unauthorised devices being connected to network machines increased the risk from malicious software.

4.22 ITSA responded to the ANAO's findings by outlining a plan to replace all non-encrypted USB flash drives in use at ITSA with secure devices, which

---

[80] The terms and conditions for use of the USB flash drives included not copying any files onto non-ITSA owned equipment, and working directly from the device while offsite. In addition, the agreement detailed password requirements, in that an incorrectly entered password will permanently erase the device after three incorrect attempts.

[81] One site support team provided evidence of a device issue register which was reportedly updated in February 2011 to track the location of their team's pooled devices. While this system would theoretically assist ITSA to monitor the use of the devices, the ANAO observed anomalies in the information provided, indicating that the process had not been adhered to closely.

will be registered as an ITSA asset and subject to yearly stock-take. ITSA also stated that it intended to implement a 'whitelisting' approach to enable only the encrypted USB flash drives to connect to the ITSA network, and log all file transfers to USB flash drives. In addition, ITSA planned to 'lock down' CD/DVD drive access, with only System Managers still having access to this function.

4.23 The work planned by ITSA, supported by appropriately reviewed policies, should address the weaknesses in ITSA's management of USB flash drives and CDs/DVDs identified in the audit.

Australian Hearing

4.24 While Australian Hearing's policies for USB flash drive and CD/DVD use were reasonably robust (see Chapter 2), there were inadequate software controls to support the policies. Australian Hearing did not have a central register of its corporately issued USB flash drives. The devices were not password protected or encrypted, meaning that if one were to be lost or stolen, any information held on the device would be easily accessible.

4.25 Further, there were no software or hardware controls preventing personal USB flash drives and CDs/DVDs from connecting to laptop or desktop computers, and transferring files to and from the network. While Australian Hearing was investigating the use of a logging program to monitor files transferred to and from the network with PSDs, this was not in place at the time of the audit.

4.26 Australian Hearing responded that it planned to replace all existing corporately-issued USB flash drives with encrypted devices. However, at the time of reporting, the agency was unsure of the suitability of 'whitelisting' to prevent personal USB flash drives connecting to its ICT network.

Test results for laptop computers

4.27 The ANAO tested agencies' compliance with a number of ISM controls for the use of laptop computers. The results for the ATO and ITSA are set out below. The laptop computers used by Australian Hearing had a number of control weaknesses which are not reported in detail here (see paragraph 4.6).

Table 4.2

ICT controls on laptop computers: ANAO testing

Criterion	ATO	ITSA
Mobile device storage encryption – ISM Control: 0869 (IC) Agencies should encrypt information on all mobile devices using at least a DSD Approved Cryptographic Algorithm.	✓	✗
Password selection policy – ISM Control: 0421 Agencies should implement a password policy enforcing an appropriate level of complexity.	✓	✓
Configuration control – ISM Control: 0863 Agencies should prevent personnel from installing or uninstalling applications on a mobile device once provisioned.	✓	✓
Use of privileged accounts – ISM Control: 0444 Agencies should ensure the use of privileged accounts is controlled, accountable and kept to a minimum.	✓	✓
User authentication – ISM Control: 1039 It is recommended agencies use multi-factor authentication for access to networks and gateways.	✓	✓
Virus protection – ISM Control: 1033 Agencies should ensure appropriate intrusion detection and virus protection.	✓	✓
Bluetooth functionality – ISM Control: 0682 (IC) Agencies must not enable Bluetooth functionality on mobile devices.	✓	✓
Media sanitisation – ISM Control: 0354 Agencies must appropriate sanitise non-volatile magnetic media.	✓	✓
Interface connections – ISM Control: 0344 Agencies should disable IEEE 1394 interfaces (for example, FireWire ports).	✓	✓

Source: ANAO testing.

Legend: ✓ indicates that the control measures adequately addressed identified risks.

⦸ indicates that the control measures partially addressed identified risks.

✗ indicates that the control measures did not adequately address identified risks.

Analysis – laptop computers

Australian Taxation Office

4.28 As identified in the table above, overall the ATO's fleet of ROAM laptops had effective controls for the secure storage and transmission of corporate information. The ANAO observed detailed assessments, design documents, and penetration test results for the agency's ROAM laptops.

4.29 Where vulnerabilities had been identified, the ANAO reviewed the actions that had been implemented by ATO to reduce or mitigate many of the identified key risks.

Insolvency and Trustee Service Australia

4.30 As required by the ISM, agencies whose ICT systems contain unclassified but sensitive information not intended for public release[82] should encrypt information on *all* mobile devices (including laptop computers), using a DSD-approved cryptographic algorithm.[83] If encryption is not possible, or does not lower the classification of the device to an unclassified level, the device should be physically transported using an approved secure briefcase.

4.31 At the time of audit fieldwork, ITSA had not implemented hard disk encryption on its laptop computers. The risk associated with a lack of hard disk encryption is if a laptop is lost or stolen, the information stored on it can be obtained by directly accessing the hard drive.[84] If the data on the laptop was encrypted appropriately it would be much more difficult for the individual to understand the information on the hard drive, significantly reducing the risk of data loss.

4.32 The ANAO recognises the possible cost implication of implementing hard drive encryption, and also that DSD is currently evaluating low-cost encryption products such as those that come as part of a SOE package, and may be available to provide individual advice to agencies on options for hard disk encryption.

---

82 *Information Security Manual 2011*, p. 2. This definition is based on the Government's new Information Classification regime announced in July 2011.

83 *Information Security Manual 2010*, p. 269 and control 0869.

84 *Information Security Manual 2010*, p. 192.

4.33 ITSA advised the ANAO that it planned to implement hard disk encryption on its fleet of laptop computers in the first quarter of 2012. A new Standard Operating Procedure (SOP) to be followed by staff responsible for issuing the laptops will include a check that encryption has been included in the machine build.

Australian Hearing

4.34 At the time of audit fieldwork the laptop computers used by Australian Hearing did not have adequate ICT control measures to meet a number of the benchmark standards as set out in the ISM.

4.35 Australian Hearing responded to the risks arising from the control weaknesses identified by the ANAO by stating that it planned to improve the ICT controls for laptop computers in a number of areas. However the agency did highlight potential difficulties in meeting all of the ISM control requirements due to their potential impact on the use of Australian Hearing medical equipment—part of the agency's core business.

4.36 The ANAO recognises the technical issues and cost implications of implementing a comprehensive ICT controls framework. However, if Australian Hearing decides not to implement ICT controls of a standard equivalent to those in the ISM for operational reasons, it would be prudent to review the type of information that is routinely stored on laptop computers when they are used 'in the field'.

Test results for smartphones

4.37 Many of the controls listed in the ISM 2010 are not specific to various types of devices, in particular those that have communication as well as storage functions. As such, they often do not provide prescriptive information to enable clear-cut tests against each control.

4.38 In relation to smartphones, the ANAO has detailed the ISM controls most relevant to specific tests performed, based on an assessment of the agency's key risks associated with that device.

Table 4.3

ICT controls on smartphones: ANAO testing

Criterion	ATO	ITSA	Australian Hearing
Mobile device storage encryption – ISM Control: 0869 (IC) Agencies should encrypt information on all mobile devices using at least a DSD Approved Cryptographic Algorithm.	✓	⦸	✗
Unauthorised use of mobile devices – ISM Control: 1086 Mobile devices should not be used by people other than those specifically authorised.	✓	✓	⦸
Registering media – ISM Control: 0946 It is recommended agencies register all media with a unique identifier in an appropriate register.	✓	✓	✓
Non-agency owned mobile devices – ISM Control: 1047 Non-agency owned mobile devices connecting to systems should use a trusted operating environment.	✓	✓	✓
Emergency destruction – ISM Control: 1050 (IC) It is recommended agencies develop an emergency destruction plan for mobile devices.	✓	✓	✓

Source: ANAO testing.

Legend: ✓ indicates that the control measures adequately addressed identified risks.

⦸ indicates that the control measures partially addressed identified risks.

✗ indicates that the control measures did not adequately address identified risks.

(IC): IN-CONFIDENCE information and system applicability.

Analysis – smartphones

Australian Taxation Office

4.39 Overall, the ATO's smartphones (BlackBerry) were well controlled with only minor vulnerabilities. The ANAO observed that the current BlackBerry configuration had been subject to a number of ATO risk assessments including against the DSD hardening guide specifications and via penetration testing.

4.40 These assessments identified several areas where the BlackBerrys contained vulnerabilities that potentially made them unsuitable for wider use across the organisation. The ANAO notes that the use of BlackBerrys within the ATO was only at the trial stage during the audit. Any expansion in the deployment of Blackberrys would be subject to an assessment to be in line with the agency's security environment.

Insolvency and Trustee Service Australia

4.41 Only ITSA-issued smartphones (Blackberry) can connect to the ITSA email and calendar system. The smartphones also allow Internet access, however they cannot be used to access files or applications from the corporate network.

4.42 The ANAO was advised that when ITSA procured the BlackBerry smartphones in 2008, it complied with DSD advice regarding security controls. The connection through the BlackBerry Enterprise Server (BES) enables the native encryption included with the smartphones and protects information sent via email. However, emails and attachments can be downloaded from the secure server onto the individual device. ITSA advised that no additional encryption to information stored on the smartphone itself had been implemented.

4.43 In addition, ITSA had no procedures in place for logging or monitoring the information transferred onto the BlackBerry smartphones, either through email, or transfers via USB connection.

4.44 Overall, the ANAO's assessment was that ITSA's current use of smartphones did not pose a significant risk to the agency. The limited numbers (13 in use at the time of the audit) and functionality of the smartphones mitigated against many of the more serious threats associated with the use of these devices. However, the ANAO suggests that ITSA examine procedures and technical mechanisms that could restrict, protect, and monitor the information transferred to, and stored on the devices.

Australian Hearing

4.45 Australian Hearing had taken a decision to allow both corporately issued and personal smartphones (mostly Apple iPhones) to connect to the corporate email network. On the whole, the ANAO considered that the controls applied to these smartphones provided sufficient security protection. Compared to the current ICT controls for Australian Hearing's laptop computers, smartphones posed less risk for a malicious attack.

4.46 The main risk in smartphones connecting to the Australian Hearing email network was that the agency did not enforce a password/PIN protection. This meant that if a smartphone were lost or stolen, an unauthorised user could access the Australian Hearing email network, potentially viewing sensitive emails and documents attached to those emails.

4.47 Australian Hearing responded that it would implement password/PIN protection for all smartphones connecting to its email network.

Use of 'personal' devices in each agency

4.48 One of the major risks of PSD use for agencies as identified by both DSD[85] and the Privacy Commissioner, is when staff are allowed to use (or choose to ignore policies which prohibit the use of) personal devices on agency systems. The inherent risks with this are that the agency has much less control over the types of devices that are connecting to its network, and associated control mechanisms such as SOE and virus updates.

4.49 While the policies in all three audited agencies prohibited or at the least discouraged the use of personal devices to store and/or transmit agency information, in interviews and the staff survey there was evidence of some use of personal devices by staff employed at all three agencies—for example, emailing documents to a personal email account and working on them with a personal laptop computer at home. These are summarised at Appendix 3.

4.50 The results indicate the existence of practices that potentially put the security of corporate information at an increased risk, and the ANAO suggests that all agencies should include a consideration of these issues as part of the risk assessments for PSDs that have been recommended in Chapter 2.

Conclusion

4.51 Appropriate ICT controls are a vital element to an effective overall approach to security for PSDs in agencies. An effective risk assessment will highlight the most appropriate controls needed in individual agencies to mitigate identified security risks. Agency ICT controls should also be in line with the Government's requirements set out in the ISM and other DSD publications such as hardening guides and formal evaluations.

4.52 Overall, the ATO had implemented ICT controls that met the requirements of the ISM and adequately addressed the risks of PSDs to that

[85] The latest version of the *Information Security Manual 2011*, discusses the potential for agencies to allow staff to use their personal devices to connect to the agency ICT system. However, the ISM states that this should only be via a Trusted Operating Environment which can ensure a secure channel, and through which information is not stored on the device itself but on secure agency servers.

organisation. However, both ITSA and Australian Hearing could improve aspects of their ICT controls framework.

4.53 The ANAO observed that a common weakness was in the ICT controls for the use of USB flash drives and CDs/DVDs. Due to their size, portability and capacity to store large amounts of data, these devices pose security risks to agencies.

4.54 ITSA's laptop computers did not have hard disk encryption at the time of the audit, however the agency advised the ANAO that all of its laptops are expected to have hard disk encryption early in 2012.

4.55 Australian Hearing laptop computers had a number of control weaknesses at the time of the audit. Australian Hearing advised the ANAO that it was working to address many of these issues, while continuing to consider the business impact of implementing other controls.

4.56 The ANAO's recommendation below is not technology or control-specific, in recognition that new technologies and devices will continue to be used by agencies. The ICT environment is rapidly evolving, and agencies will increasingly need to assess the risks posed by these new technologies, including the appropriateness and security challenges associated with incorporating their use into agency operations.

Recommendation No.3

4.57 The ANAO recommends that agencies implement hardware and software controls for Portable Storage Devices that mitigate identified security risks.

ITSA response

4.58 Agreed. ITSA has implemented hardware and software controls for PSDs. This includes 'white listing' devices that can be connected to USB ports, providing secure encrypted USB drives to staff, providing a register to each site for recording usage, removing non-secure PSDs and removing the 'write' permissions to CDs and DVDs. ITSA has sourced software to encrypt hard disk drives on both laptop and desktop computers and this will be implemented during the first quarter 2012.

Australian Hearing response

4.59 Australian Hearing accepts Recommendation 3 and has already started investigating possible controls for the safe use of PSDs. The evaluation of possible PSD control solutions will be undertaken to identify the best fit solution for AH's needs with acknowledgement of the Protection Profiles and Evaluated Products List published by the DSD to be completed Q3-Q4 2012/13.

5. Staff Training and Awareness

This chapter examines the audited agencies' activities to ensure staff awareness of the security and privacy risks associated with Portable Storage Devices.

The importance of staff training and awareness activities

5.1 A key element in any organisation's security practices is the people who work for and interact with that organisation. A recent Western Australia Auditor-General's report (outlined below) highlighted how easily existing security mechanisms can be undermined. The Auditor-General stated:

> Employees can pose the biggest risk to information security and bypass all other security mechanisms. This weakness can undermine the security requirements for agencies and lead to the compromise of systems.[86]

Figure 5.1

Western Australian Auditor-General: Social engineering

As part of an audit released in June 2011, the Western Australian Auditor-General used social engineering techniques to test a number of Western Australian public sector agencies, in particular staff awareness, policies, and incident response processes in place for potential threats.

One test was the ability and willingness of agency employees to plug non-agency USB flash drives (USBs) or other devices into internal ICT networks, in areas not normally accessible by the public.

The WA Audit Office deployed 25 USBs across 15 agencies, in public and 'behind the counter' areas. These USBs did not contain auto-executing malware but instead relied on a 'social approach'. An individual would have to plug in the USB, then make a decision to read a file and run a program. The message contained within the file and the steps required to run the program should have been sufficient to make an individual suspicious and wary. If activated, the USB 'phoned home' telling the WA Audit Office where it was, and sent some basic network information.

Staff from eight agencies plugged in and activated the USBs. The USBs sent information back to the WA Audit Office via the Internet. This type of attack can provide ongoing unauthorised access to an agency network and is extremely difficult to detect once it has been established.

Source: Western Australian Auditor-General and ANAO.

[86] Western Australian Auditor-General's Report: *Information Systems Audit Report*, Report 4 – June 2011, Western Australian Government, 2011.

5.2 The importance of training and awareness programs in enabling agencies to build a security culture is paramount, as highlighted by the Attorney-General in a speech to government ICT officers in August 2011:

> From agency heads down, all staff need to understand, prioritise and manage security risks. Agencies can only achieve effective protective security if security is part of the agencies' culture, practices and operational plans. One way to improve an agency's security culture is by raising employee awareness of the possible risks…you have an obligation to educate your own staff about the possible consequences of ignoring good security practices.[87]

5.3 Similarly, DSD has recognised the importance of training and awareness programs in its latest release of the *Strategies to Mitigate Target Cyber Intrusions* (2011). 'User education' was elevated to number eight in the 2011 list (up from number 31 in 2010). DSD ranks user education as an excellent security measure, in particular education that covers:

- most likely targets, about Internet threats such as identifying spear phishing, socially engineered emails or unexpected duplicate emails, and reporting such emails and suspicious phone calls to the security team;
- the dangers of: selecting weak passphrases, reusing the same passphrase on the same system, using the same passphrase in several different places, unnecessarily exposing email address and other personal details, visiting web sites unrelated to work, and using USB devices and other IT equipment not corporately provided; and
- why following IT security policies helps to protect and appropriately handle the sensitive information that users have been entrusted to handle.[88]

5.4 The ANAO Audit Report No.25 2009–10 *Security Awareness and Training*[89] examined the security and awareness programs in four government

---

87 The Hon. Robert McClelland MP, Attorney-General, *Speech to the Technology in Government and the Public Sector Summit*, 8 August 2011, available at: <http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2011_ThirdQuarter_8August2011-TechnologyingovernmentandthePublicSector#>, [accessed 26 September 2011].

88 DSD, *Strategies to Mitigate Targeted Cyber Intrusions – Changes*, 12 July 2011, available at: <http://www.dsd.gov.au/publications/Top_35_Mitigations_Changes.pdf>, [accessed 21 September 2011].

89 ANAO Audit Report No.25 2009–10 *Security Awareness and Training*, Commonwealth of Australia, April 2010.

agencies and identified better practice examples to assist agencies in strengthening their security culture.

5.5 The PSPF has a mandatory requirement for agencies to provide security training and awareness programs, and the Privacy Commissioner's guidance offers some specific advice to agencies about effective training on the risks associated with PSDs, and security procedures. The Commissioner's 2009 survey indicated that most agencies provided training for staff on the use of agency-issued PSDs in the form of on-the-job training.

Figure 5.2

Protective Security Policy Framework and *Information Security Manual*: Training and Awareness Programs

PSPF GOV 1 – MANDATORY

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.

PSPF *Security Awareness Training Guidelines*[90]– guidance for agencies about how to effectively implement a training and awareness program.

ISM Control: 1083 – MUST (UNCLASSIFIED and above)

Agencies must advise personnel of the maximum permitted classifications for data and voice communications when using mobile devices.

Source: Protective Security Policy Framework and *Information Security Manual 2010*.

[90] *Protective Security Policy Framework*, *Security Awareness Training Guidelines* September 2010, available at: <http://www.ag.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads>, [accessed 15 June 2011].

Figure 5.3

Privacy Commissioner: Issues to be included in PSD training programs

Key issues to be included in training:

Where possible, an initial training session should occur before issuing staff with a PSD and at regular intervals afterwards.

Risks: Outline the inherent privacy risks associated with using PSDs to handle personal information.

Policy: Provide staff with a hard copy of the policy, and show them where to find it electronically. Also, highlight key parts of the policy applying to staff, including personal responsibility, acceptable use and what to do when a PSD is lost or stolen.

Software and hardware controls: Describe any applicable software controls applying to the use of agency issued or privately owned PSDs, or hardware controls affecting privately owned PSDs.

Contacts: Provide staff with a list of contacts in the IT or Personnel areas, who can assist staff with any issues associated with PSDs.

Consider asking staff to sign an 'Acceptable Use Agreement' at the end of training sessions, which confirms that staff understand and consent to their obligations and responsibilities.

Conduct ongoing activities such as reminders during staff meetings, email or staff bulletin reminders, computer logon banners.

Source: Privacy Commissioner's guidance, op.cit.

Agencies' training and awareness activities for the use of Portable Storage Devices

Methodology

5.6 The ANAO examined whether agencies actively promoted staff awareness of the security and privacy risks associated with the use of PSDs. This included a review of training programs and other staff communication activities, interviews with staff in each agency, and an online survey of selected agency staff, which included questions regarding their understanding of agency policies, participation in training activities, and their opinion of the effectiveness of their agency's training and awareness activities.

5.7 Agencies were expected to have a current security training program that covered the risks associated with the use of PSDs, as required by the PSPF and ISM outlined in Figure 5.2 above. In addition, better practice would see

supporting awareness activities such as team briefings, staff emails/newsletters and other communication activities.

Australian Taxation Office

Induction training

5.8 The ATO has an in-house online training tool used for agency-wide programs such as induction training and corporate policies. The two most relevant online training programs for this audit were *Security Privacy and Fraud*; and *Security Essentials*. These programs are part of the ATO induction package. ATO reported that at 31 March 2011, over 95 per cent of all staff had completed these two programs, and they are rolled out to all staff as a refresher course on a two-yearly basis.[91]

5.9 The ATO induction courses provide a sound introduction to security issues generally, and some specific advice relating to the use of PSDs, in accordance with the majority of the Privacy Commissioner's guidance outlined in Figure 5.3.

Other training and awareness activities

5.10 Apart from the induction program, specific training on the use of PSDs is the responsibility of team managers. Some materials are provided to ATO users when they are issued with a PSD (for example, an email to staff assigned a ROAM computer, with links to relevant policies).

5.11 The ANAO reviewed a number of materials developed in individual business lines or teams for the use of particular PSDs—for example USB flash drives or ROAM laptops. These materials outlined the appropriate uses for the devices, associated risks, and responsibilities for ATO users including reporting for security incidents including lost or stolen devices.

5.12 The ANAO suggested that these more specific training materials be located in a central depository on the ATO intranet, and deployed across the organisation as appropriate. The ATO agreed to this suggestion, where possible and appropriate.

[91] The ATO's human resource management system records all staff training activities, and automatically prompts staff members and their managers that they are due for refresher courses such as the *Security Essentials* program.

5.13 The other major avenue for communication of security and other key messages at the ATO is via the Manager Assurance Program (MAP). The MAP is designed to:

- provide assurance to ATO Executive about managers' awareness of their obligations;
- create and store evidence relating to Certificate of Compliance requirements; and
- disseminate corporate information to the wider ATO staff base via regular team meetings.

5.14 The MAP process generally involves an online survey of ATO managers (usually EL2 and some EL1[92] staff), which is conducted monthly, quarterly or bi-annually (depending on the business line). These surveys reach over 3 500 ATO managers at least twice every year.

5.15 The questions are not the same across all ATO areas, or in each survey. A rolling program of questions reflects key messages for each particular area, or covers issues on which the ATO Executive has requested assurance coverage.

5.16 Many questions ask managers to verify that they have briefed their staff regarding legislative requirements and/or ATO policies and procedures. Because of this, the MAP process incorporates staff meetings either formally or informally.[93] Over a 15-month period leading up to the audit fieldwork, the MAP surveys deployed across the ATO included a total of 48 questions[94] relating to management of PSDs.

5.17 Results of the ANAO's survey of ATO staff showed that of the 322 staff who answered the question on PSD training, only 44 (13.7 per cent) indicated they had received no training from any source on the use of PSDs.

---

92 EL refers to Executive Level staff. This is a common term across the Australian Public Service, and sits below the Senior Executive Service level.

93 For example, the one area's MAP process formally incorporates staff meetings by publishing a team meeting template agenda every month. The matters for discussion in the template agenda will include topics raised in that month's MAP survey.

94 As the MAP process is managed differently in each sub-plan, not all surveys would have included 48 questions over the 15 month period. This is the aggregate number across the entire agency.

5.18 On a scale of 1 ('very useful') to 5 ('not at all useful'), each of the following sources of training or advice were rated as either 1 or 2 by a large percentage (between 80 to 90 per cent) of the staff who had received the training or advice.

- formal security training or advice;
- informal security training or advice;
- agency newsletters and/emails; and
- agency intranet page.

5.19 Most free-text responses also indicated that the ATO had provided staff with training and other awareness advice about PSDs, for example:

> …the advice received generally alerts an employee as to their on-going responsibility for devices and directs the employee to more specific sources of instruction.

5.20 These results support the ANAO's assessment that the ATO generally has a well-developed and effective security training and awareness framework.

Insolvency and Trustee Service Australia

5.21 The most structured approach to security awareness training in place at ITSA was via the induction training program. The induction package is tailored to staff in various employment circumstances (new to the APS, returning from long-term leave etc).

5.22 Management staff interviewed by the ANAO advised that they also delivered informal, on-the-job training to new staff. This training provided information to new employees regarding the specific roles and operations of their team, which may include coverage of ICT security practices at the team level.

5.23 In addition to the induction training, there had been one protective security training program conducted at ITSA in the period 2009–2010. This training program provided a comprehensive background to protective security within ITSA, including coverage of the appropriate use of PSDs. However, the training program had not been delivered to ITSA staff in the 12 months prior to the audit. There appeared to be no structured security training framework at ITSA and there were no records of which ITSA staff had completed security training.

5.24 The ANAO's survey of ITSA staff showed that of the 66 staff who answered the question on PSD training, only five indicated they had received 'formal security training or advice' in the last two years regarding the use of PSDs. Thirty-two staff indicated that they had not received training from any source on the use of PSDs. These survey results support the ANAO's conclusion that ITSA's security awareness and training framework could be improved.

5.25 Free text responses to the survey also indicated a need for training programs, for example:

> [I] would like refresher training, and will be reviewing the relevant policy and making sure colleagues are familiar with it. The organisation has on a couple of occasions during the last two years provided reminders to staff about policies regarding internet and email usage.

5.26 ITSA responded to the ANAO's conclusions by advising that as part of its program of work to address the risks associated with the use of USB flash drives, all staff will be given training in the use and risks of PSDs. This training will include examples outlining the impact of devices being lost or stolen, the classification of data and emails, ITSA's *Acceptable Use of ICT Resources*, and the actions to be taken by staff when a device goes missing.

5.27 ITSA also advised that its induction process will be amended to include information on classifying data and the protection of data both on ITSA premises and if taken off site or to client sites.

Australian Hearing

5.28 The most structured approach to security awareness training in place at Australian Hearing during the audit was via the induction training program. A centralised induction package for new Australian Hearing staff was attended face-to-face by National Head Office staff, while non-National Head Office staff worked through a paper-based package of induction materials. The existing induction materials included modules on privacy, confidentiality, IT Security and email, Internet and electronic access policies.

5.29 Apart from the induction training, there had not been a regular security awareness training program in place at Australian Hearing in the past several years. While some ad-hoc training may have been undertaken at the local levels, there was no record of this training or of which staff may have completed it.

5.30 At the time of fieldwork, Australian Hearing was implementing a centralised training management system, replacing the previous arrangements under which most training was planned and conducted in the various Australian Hearing regions and Australian Hearing Centres. Australian Hearing advised the ANAO that the new training system would include security awareness programs with modules on security for PSDs, and staff attendance will be tracked in the new system.

5.31 Results of the ANAO's survey of Australian Hearing staff showed that of the 227 staff who answered the question on PSD training, only ten indicated that they had received 'formal security training or advice' regarding the use of PSDs.

5.32 While most staff indicated that they had received 'other' training or advice from sources such as their managers, newsletters, emails, or the intranet, 51 (22.5 per cent) indicated they had not received training on the use of PSDs from any source. Some free text responses from survey reflected this, for example:

> Most information regarding policies of this nature or similar are emailed [to us], but no formal training is provided.

5.33 The survey results indicate that in addition to implementing the formal training system outlined above, Australian Hearing could improve its use of 'informal' communication systems to see that key messages about security, including that for PSDs, are effectively promulgated to all staff.

Conclusion

5.34 The mandatory requirements of the PSPF and ISM, and the Privacy Commissioner's better practice guidance, all recognise the importance of training and awareness programs in enabling agencies to build a security culture.

5.35 The ATO had a comprehensive security training and awareness program that covered the risks associated with the use of PSDs. The ANAO found that ITSA and Australian Hearing could improve their approach to security training and awareness in their organisations. While each agency had some training programs and/or materials in place, there was no coordinated approach to security training and awareness in general or, specific to this audit, regarding the agencies' expectations of their staff for the use of PSDs.

Recommendation No.4

5.36 The ANAO recommends that agency security training and awareness programs address the risks of Portable Storage Devices to their organisation.

ITSA response

5.37 Agreed. ITSA has developed and promulgated security awareness presentations to all staff regarding the use of PSDs. An 'all staff' message has been sent out via email and is on the intranet. Presentations have been developed for site leaders to present to staff and these presentations will be completed before the end of December 2011. Comprehensive training on all aspects of ITSA's ICT usage and security arrangements are planned for March 2012.

Australian Hearing response

5.38 Australian Hearing accepts Recommendation 4 and will engage the Learning and Development department to make use of the existing Australian Hearing Online Learning Management System to prepare and deliver staff training to increase awareness around the risks and responsibilities involved with PSDs. To be in place by end Q1 2012/2013.

Figure 5.4

Better Practice Example: Staff communication and compliance framework

Australian Taxation Office: Manager Assurance Program (MAP)

The MAP uses an online survey tool to provide assurance to the ATO Executive that managers (usually EL1 or EL2 level) are aware of ATO policies and procedures and have briefed their staff on these requirements. Key elements of the MAP program are:

- an online survey of ATO managers conducted at regular intervals;
- survey questions based on key messages that the ATO Executive wishes to promulgate to staff and/or receive assurance on;
- many questions ask managers to verify that they have briefed their staff regarding legislative requirements and/or ATO policies and procedures;
- in some ATO line areas, the MAP process includes team meeting agendas that are based on the key questions in the current survey; and
- review of survey results by relevant ATO Executive.

The ANAO noted that over the past year there had been a number of questions in the MAP process particularly relating to the use and management of PSDs.

While the MAP online survey process is particularly suited to larger government agencies, some elements of the process could be adapted by other agencies, particularly the process by which key messages from Executive are promulgated via managers to teams throughout the organisation.

Source: Australian Taxation Office, advice provided to the ANAO.

6. Lost and Stolen Portable Storage Devices

This chapter examines agencies' mechanisms for reporting and response in the instance of a lost or stolen Portable Storage Device.

The impact of theft and loss of devices

6.1 Given their size, portability and the 'attractiveness' of PSDs, it is highly likely that some devices owned by agencies will be lost or stolen. While there is a monetary cost every time a PSD is lost or stolen, of equal or greater concern is the type of information that the device may hold, and whether it can be easily accessed by an unauthorised person.

6.2 The potential impact from unauthorised access to government information could include compromise to national or agency security, information about government decision-making (for example Cabinet-in-Confidence or budget materials), commercial information, and personal information. In addition, data loss may result in reputational damage to the government as a whole or the individual agency involved, or be used to cause disruption or damage to an organisation's ICT and security environment.

6.3 As outlined in Chapter 1, media reports over a number of years have highlighted cases in which PSDs containing sensitive information have been lost or stolen from Australian and international government agencies.

6.4 It is difficult to gain an accurate picture of the number of government PSDs that are lost or stolen in any given year. The Australian Institute of Criminology (AIC) reported on the theft of telecommunications and computer equipment (including mobile devices) in its report *Fraud Against the Commonwealth* (2008–09).[95] That report found that 29 per cent of all agencies surveyed by the AIC had experienced theft of telecommunications and computer equipment by an external source (amounting to a total number of 3,495 incidents). Sixteen agencies reported this type of theft by an internal source, amounting to a total number of 70 incidents.[96]

[95] Australian Institute of Criminology, *Fraud Against the Commonwealth 2008-09 Annual Report to government*, Prepared by Jade Lindley and Russell G Smith, AIC Monitoring Report 14, 2011.

[96] Australian Institute of Criminology, op.cit., pp. 21 and 30.

6.5 The ANAO notes that the AIC figures above include **all** telecommunications and computer equipment, not just the PSDs included in this audit. The AIC figures also do not cover lost equipment.

6.6 In 2004 the Joint Committee of Public Accounts and Audit (JCPAA) highlighted the loss and theft of laptop computers in particular, finding that in the period from 1998–2003, at least 1 000 government laptops had been lost or stolen.[97]

6.7 In the Privacy Commissioner's 2009 survey of 94 government agencies[98], over half reported that they had experienced the loss or theft of an agency-issued PSD over the previous 12 months. Nearly all the agencies were able to estimate the number of PSDs lost or stolen. For over half of the agencies this number was between two and 10. However, 16 per cent reported that over 10 PSDs were lost or stolen in the previous 12 months, and one large agency reported that it had lost over 200 PSDs.[99]

6.8 The PSPF and ISM both have some mandatory requirements for incident response, outlined below.

---

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

98 The Office of the Privacy Commissioner sent the survey to 118 government agencies, and received 94 responses. This represented an 80 per cent response rate.

99 The Office of the Privacy Commissioner, *Portable Storage Devices and Australian Government Agencies*, Personal Information Survey, April 2009, available at: <http://www.privacyawarenessweek.org/paw/documents/psd_report.pdf>, [accessed 21 June 2011].

Figure 6.1

Protective Security Policy Framework and *Information Security Manual*: Incident response procedures

PSPF PHYSEC 2 – MANDATORY

Agencies must have in place policies and procedures to report incidents to management, human resources, security and law enforcement authorities, as appropriate; and maintain thorough records and statements on reported incidents.

PSPF PHSYEC 6 – MANDATORY

Agencies must implement a level of physical security measures that minimises or removes the risk of ICT equipment and information being made inoperable, or being accessed, used or removed without appropriate authorisation.

ISM Controls: 0122, 0125, 0139, 0123 – MUST/SHOULD (UNCLASSIFIED and above)

Agencies must detail cyber security incident responsibilities and procedures for each system.

Agencies should ensure that all cyber security incidents are recorded in a register.

Agencies must direct personnel to report cyber security incidents to an ITSM as soon as possible after the cyber security incident is discovered.

Agencies must report significant cyber security incidents[100] to DSD.

It is recommended that agencies report non-significant cyber security incidents to DSD.

Source: Protective Security Policy Framework and *Information Security Manual 2010*.

6.9 The Privacy Commissioner has published some guidance for agencies about handling personal information data breaches. These guidelines also represent better practice for a wider spectrum of data breaches that may be the result of lost or stolen PSDs. There is currently no specific requirement in the Privacy Act to notify individuals when and if a breach has occurred (a 'data breach'), including a lost or stolen PSD.[101] However, the Government is considering an Australian Law Reform Commission recommendation to

[100] The theft or loss of any device that might have been, or has been used to either process or store government information, is considered to be a 'significant cyber security incident'. DSD, *Onsecure* website (login required).

[101] The Office of the Privacy Commissioner, *Guide to handling personal information security breaches,* August 2008, available at: <http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=guidelines&fullsummary=6478&Itemid=1021>, [accessed 21 August 2011].

introduce data breach legislation, as part of a wider package of reforms to the Privacy Act.[102]

6.10 The Privacy Commissioner's guidance outlines four key steps in responding to a breach.

Figure 6.2

Privacy Commissioner: Four key steps in handling personal information security breaches

Step 1: Contain the breach and do a preliminary assessment—take steps immediately to contain the breach, if possible, and quickly appoint a person to lead the initial assessment.

Step 2: Evaluate the risks associated with the breach—evaluate who or what systems are affected by the breach, what is the context of any personal information involved, and consider how the information could be used.

Step 3: Consider notification—consider whether notification to an individual is necessary in order to avoid or mitigate serious harm to that individual, notify as soon as possible if it is considered necessary, outline the agency's response to the breach, offer assistance if possible, provide contact details for further questions.

Step 4: Prevent future breaches—review current policies and procedures to identify any gaps that resulted in the current data breach, implement necessary changes, review staff training and awareness programs and update to reflect new identified risks.

Source: Office of the Privacy Commissioner, *Guide to handling personal information security breaches, August 2008*.

Agencies' incident response procedures

Methodology

6.11 To assess agencies' reporting and response mechanisms for lost and stolen devices, the ANAO reviewed policies and procedures, reviewed incident reports, tested relevant ICT controls, interviewed agency staff, and surveyed selected agency staff with questions including their understanding of

[102] The data breach notification changes would be part of the second package of reforms to the Privacy Act, which will be considered by the Government once the first package of reforms have been implemented. An exposure draft of new legislation, including revised Australian Privacy Principles, has been released and was considered by a Senate committee in 2011 (see the Senate Finance and Public Administration Committee at: <http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/index.htm>. However at the time of this report, the timing for Parliamentary consideration of the proposed legislation was unclear. See the PM&C website: <http://www.dpmc.gov.au/privacy/reforms.cfm>, [accessed 4 November 2011].

their responsibilities in the case of a lost or stolen device. Agencies were expected to have in place:

- a register of the PSDs authorised for use in their organisation including which staff were assigned a particular device;
- a documented response mechanism in the case of theft or loss of a PSD which included reporting to the appropriate stakeholders including DSD; and
- a logging program which allowed the agency to track what data is contained on a particular device (better practice).

Register of Portable Storage Devices

6.12 As outlined above, the ISM recommends that agencies register PSDs with a unique identifier.[103] According to the ISM:

> If agencies fail to register media with an appropriate identifier they will not be able to effectively keep track of their classified media and there will be a greater likelihood of unauthorised disclosure of classified information.[104]

Australian Taxation Office

6.13 ATO staff may only be granted use of a PSD via an online request which is endorsed by their manager. The ATO had a register in place for all authorised PSDs. The register included authorised users of ROAM laptop computers, USB encrypted flash drives, Blackberry smartphones, portable external hard drives, and staff granted 'write' access on the CD/DVD drive.[105]

Insolvency and Trustee Service Australia

6.14 ITSA's laptop computers and smartphones were assigned unique identifiers, kept on the agency's asset register and included in the agency's stock-take procedures. However, the same controls were not in place for the management of USB flash drives or CDs/DVDs.

---

[103] This is a 'Should' control for information that is marked 'CONFIDENTIAL', 'SECRET/HIGHLY 'PROTECTED', and 'TOP SECRET' (Control 0336).

[104] *Information Security Manual 2010*, op.cit., p. 152.

[105] All ATO staff may read CDs and DVDs and transfer files onto the ATO network, provided these files fall into the category of 'restricted' file types – for example, word documents, PDF files, etc. Executable files cannot be transferred onto the network. All file transfers from a CD/DVD first pass through the ATO's virus detection program and the transfers are logged.

6.15 At the time of audit fieldwork, some ITSA USB flash drives and CDs/DVDs were purchased as 'consumables' with other stationery items. There were different register or loan requirements for USB flash drives across the organisation. The ANAO also observed that the loan registers were not always well maintained.

6.16 However, in December 2011 ITSA informed the ANAO that it was in the process of purchasing a number of encrypted USB flash drives that would replace the existing devices. Only these authorised devices will be allowed to connect to the ITSA network.

Australian Hearing

6.17 Australian Hearing had a register for its laptop computers and agency-issued smartphones. However, there was no register for USB flash drives or CDs/DVDs. As outlined in Chapter 4, there were limited controls on the use of USB flash drives—for example, agency-issued USB flash drives did not have encryption or password protection, and there was no logging of connections to the network. A well-maintained PSD register would enable Australian Hearing to effectively keep track of its PSDs and assist investigations into lost and stolen devices and associated data spills.

Incident response and reporting mechanisms

6.18 Agencies are required to report any lost PSDs to DSD. There may also be a need to report a stolen device to the Australian Federal Police (AFP), depending on the monetary value of the item, or if the agency suspects fraud. There are also some better practices (outlined in Figure 6.2) that agencies should follow in order to ascertain what type of information may have been compromised, and mitigate associated risks as far as possible.

Australian Taxation Office

6.19 As outlined in Chapter 3, ATO security policies, including those specifically regarding PSD use, provide instructions to staff about what to do if their device is lost or stolen. The ATO Intranet includes a Security page through which staff can lodge a security incident report. There is also a phone number available 24 hours a day. As would be expected in a large agency, the ATO had a dedicated Security Policy and Service section responsible for managing the ATO's security incident response procedures.

6.20 The procedures reviewed by the ANAO were clear and provided some practical examples for Security Policy and Service staff to follow (for example,

documents left on a plane, threat to an employee). The procedures included actions to ascertain what data was contained on the lost device, and possible mitigation strategies. The procedures also included reporting requirements to DSD and other stakeholders as necessary.

6.21 After the initial response is finalised, the procedure includes a Post Incident Evaluation and record keeping. The ANAO reviewed a number of incident reports. These related to lost or stolen laptop computers and did not result in changed policies or procedures. However, the ATO advised that it has previously changed policies and procedures in the wake of security incidents, and regularly uses the incident reports to generate staff awareness activities such as newsletter articles or email reminders.

Insolvency and Trustee Service Australia

6.22 The policies reviewed by the ANAO contained advice for ITSA staff about required actions if their device was lost or stolen. As outlined in Chapter 3, these policies were significantly out of date, however the ANAO acknowledges that they were under review at the time of the audit. The new policies should continue to provide clear instructions to staff about the required response if their device is lost or stolen.

6.23 The ANAO did not see evidence of internal procedures, such as ICT Standard Operating Procedures, that provided a security incident response framework, including a procedure for relevant officers to respond in the case of a lost or stolen PSD. There was no recorded procedure for reporting lost or stolen PSDs to DSD or other stakeholders as necessary.

Australian Hearing

6.24 Australian Hearing PSD policies generally included instruction for staff about their reporting requirements if their device was lost or stolen. The agency also had an asset management procedure for use by ICT support staff, which gave a high-level overview of the required response to a lost or stolen device. However, the procedure did not go into adequate detail regarding appropriate incident response, including DSD reporting requirements or responding to a potential data spill.

Logging programs

6.25 There are software technologies available that enable agencies to log and review information transferred to and from PSDs. This enhances agencies' ability to respond to security incidents, by providing an accurate record of the

information contained on the lost or stolen device. It may also help to discourage and detect inappropriate behaviour such as transferring inappropriate material onto the corporate network. The ANAO recognises that the benefits provided by these types of software must be weighed against their costs and any impact to the operation of the ICT system (for example, full recording or 'shadowing' of all files copied to and from PSDs may slow down system functionality and result in large amounts of data requiring adequate storage).

Australian Taxation Office

6.26 The ATO's logging software keeps details of any file which has been transferred to or from a PSD to the ATO network. In the case of a lost or stolen PSD, the ATO can review the logs and see which files the particular device contained. While the standard logging only records the user, file names, and file size, if an ATO staff member is suspected of unauthorised activities, 'shadowing' of that staff member's actions on the ICT network can be enabled.[106]

Insolvency and Trustee Service Australia

6.27 ITSA did not have a logging program at the time of audit fieldwork, however the agency subsequently advised the ANAO that it was considering implementing appropriate software.

Australian Hearing

6.28 Australian Hearing had not implemented a data transfer logging program at the time of the ANAO's fieldwork. However, Australian Hearing subsequently advised that it intends to introduce a logging program as part of a SOE upgrade currently underway.

6.29 The ANAO notes that the current Portable Storage Device policy states 'All data copied to/from a device is logged (recorded) for audit purposes. This information details the date/time, user, machine, device, file (name and content) and location copied from/to.' This is not currently the case at Australian Hearing. While the statement may act as an effective 'deterrent' to

[106] The data logs are kept for a 12-month period. The ANAO reviewed the logging program and sighted logs of data transfers to and from PSDs. 'Shadowing' involves copying all files accessed by a particular ATO user to a secure folder for review. Shadowing is not used for all ATO employees because it would create unmanageable volumes of data.

staff not using PSDs appropriately, it should be removed from the policy until a logging program is actually implemented.

Conclusion

6.30 Incident response procedures are an important part of any agency's security management framework. These procedures document the steps to be undertaken in an agency in the event of a security incident (physical, personnel or information security). In an ICT security and more specifically, PSD security context, an incident response procedure should outline the expected responses both from general agency staff and the officer/s assigned responsibility for managing security incidents.

6.31 Without an adequate incident response plan, agencies may be inadequately prepared to deal with incidents. The possible consequences of this unpreparedness are that decisions may be made in haste, potential risks of the incident are not identified, there is inadequate management or escalation of the incident, there is inappropriate reporting both internally and to external stakeholders, and a failure to learn from mistakes and incorporate better practices into agency business processes.

6.32 Agencies' incident response procedures should include steps to respond in the case of a lost or stolen PSD. This would start with an adequate register of agency PSDs, through to documented procedures for incident response, and possibly a logging program to assist with identifying what information may be contained on a lost device (or identifying staff who may be inappropriately removing agency information).

6.33 In each agency, policies and procedures gave clear advice to staff about their reporting obligations in the case of a lost or stolen device. However, ITSA and Australian Hearing did not have adequately documented procedures that detailed the incident response steps required of responsible officer/s.

6.34 Another element that was not addressed by these two agencies was the reporting of lost or stolen devices to DSD. While individual incidents may appear innocuous, DSD has explained that it uses these reports to identify and respond to trends across government, and to develop new policies, procedures, techniques and training measures.[107]

[107] *Information Security Manual 2011*, p. 68. All agencies should consider becoming members of DSD's *Onsecure* website, which provides an online incident reporting tool and detailed security advice.

Recommendation No.5

6.35 The ANAO recommends that agency incident response procedures cover the theft and loss of Portable Storage Devices, including Defence Signals Directorate reporting requirements and the Privacy Commissioner's better practice guidelines.

ITSA response

6.36 Agreed. ITSA has developed a PSD Incident Reporting Framework which includes the Privacy Commissioner's better practice guide and complies with the DSD reporting requirements. This document is provided to all staff who are issued with a USB storage device.

Australian Hearing response

6.37 Australian Hearing accepts Recommendation 5 and has commenced assembling a security incident response team in line with the rational laid out in the DSD ISM. The incident response team will be chartered with developing and preparing a response plan for the case where any risks identified in the risk assessment are realised. To be in place by end Q1 2012/13.

Ian McPhee
Auditor-General

Canberra ACT
20 December 2011

Appendices

Appendix 1: Background information on the audited agencies

The Australian Taxation Office

The Australian Taxation Office (ATO) is a statutory authority operating under the *Financial Management and Accountability Act 1997* (the FMA Act). The ATO administers Australia's tax and superannuation systems and has a network of 39 metropolitan, regional and outpost field offices, employing over 25 000 people.[108] The ATO is organised into four sub-plans: Compliance; Corporate Services and Law; Enterprise Solutions and Technology; and Operations. The business and service lines are the delivery arms of each of the relevant sub-plans. Each business or service line focuses on a type of taxpayer such as small business; a type of tax such as goods and services tax; or an aspect of internal support such as information technology.[109]

The ATO was selected for the audit as it collects and stores a large amount of personal information from both individuals and businesses, including name, address, date of birth, financial and banking details and tax file numbers.

Review of ATO information security

In 2008 the ATO released a review by PricewaterhouseCoopers (PwC) of its information security practices.[110] The review was commissioned by the ATO in the wake of information breaches by the UK tax office, and minor breaches at the ATO including the theft of a briefcase containing information about two taxpayers.[111] The review found that as an organisation, the ATO was highly conscious of information security. However, there were a number of areas for improvement.[112] The PwC review made a total of 22 recommendations for

---

[108] Australian Taxation Office (ATO), *Annual Report 2010-11*, Commonwealth of Australia, 2011.

[109] ATO internet site: *About Us / Organisational Structure*, available at: <http://www.ato.gov.au/corporate/content.aspx?doc=/content/24463.htm&pc=001/001/002/018&mnu=39504&mfp=001/001&st=&cy=>, [accessed 23 August 2011].

[110] PricewaterhouseCoopers, *Australian Taxation Office, Information Security Practices Review*, April 2008, p. 2. Available at: <http://www.ato.gov.au/content/downloads/COR138560InfoSecurity.pdf>, [accessed 22 July 2011].

[111] ATO, Media release: *Tax office announces information security review*, available at: <http://www.ato.gov.au/corporate/content.aspx?doc=/content/00112983.htm>, [accessed 4 November 2011].

[112] PricewaterhouseCoopers, *Australian Taxation Office, Information Security Practices Review,* op.cit.

improvement, including ten 'priority' recommendations. Relevant to this audit, the review made the following priority recommendation:

> [The ATO should] provide solutions for secure transportation of information of all types to ensure that all employees who have a requirement for such a solution have ready access to it. This may include, for example:
>
> - SCES endorsed briefcases and portable document shredders;
> - Personal electronic devices – including risk based consideration of the controls required to permit transfer and storage of information between such devices and the Tax Office at various security classification levels;
> - USB memory devices – including endorsing the interim USB Drives as a more permanent option;
> - Encrypted and hardened laptops – including consideration of controls to protect information stored on laptop hard drives and the security of communications channels that permit remote access to the Tax Office network; and
> - Secure telephone/video conferencing facilities.[113]

The Commissioner of Taxation, Mr Michael D'Ascenzo AO, stated that the priority recommendations would be implemented over the next two years. An ATO Internal Audit (July 2011) reviewed the implementation of the PwC recommendations. In addition, in 2010 the ATO conducted a staff-wide survey on security culture, to follow up on the 2008 findings and benchmark changes.

After the publication of the PwC review, a media article detailed an incident where a CD containing the details of over 3 000 self-managed super funds, including tax file numbers, went missing in transit between a printing company and the ATO.[114]

ATO's ICT environment

According to its Annual Report, the ATO has one of the largest information technology operations in the Australian Public Service, with a workforce of 2 100 people and an annual ICT operating budget of approximately

---

[113] ibid., pp, 45–46.

[114] 'CD with 3,000 taxpayer details goes missing' *ZDnet*, 30 October 2008. Available from: <http://www.zdnet.com.au/cd-with-3-000-taxpayer-details-goes-missing-339292931.htm>, [accessed 5 December 2011].

$633 million. The ATO works with external service providers to deliver and support 750 ICT systems across 61 sites nationally.[115]

Following the 2008 PwC review, the ATO implemented new technologies to assist with working away from the office, including:

- a rollout of new laptop computers with improved security settings (Roving Office ATO Mobility—ROAM);
- encrypted biometric USB flash drives;
- a trial of Blackberry smartphones for a small number of (mainly SES) officers; and
- lock-down of the CD/DVD write function—provided on an exception basis after assessment of the business need.

Insolvency and Trustee Service Australia

The Insolvency and Trustee Service Australia (ITSA) is an executive agency in the Attorney-General's portfolio. ITSA administers and regulates Australia's personal insolvency system.

ITSA is responsible for administering the *Bankruptcy Act 1966* (the Bankruptcy Act) and its related legislation, the *Bankruptcy (Estate Charges) Act 1997*. The Bankruptcy Act creates the roles of Inspector-General in Bankruptcy, Official Receiver and Official Trustee in Bankruptcy. ITSA's Chief Executive fulfils each of these roles.

ITSA's Chief Executive reports to the Attorney-General and, in accordance with the *Public Service Act 1999* and the *Financial Management and Accountability Act 1997* (FMA Act), assists the Attorney-General to fulfil their accountability obligations to the Parliament.

ITSA regulates bankruptcy private trustees and administrators, and in its role as Official Trustee, also directly provides bankruptcy and other personal insolvency services to individuals when a private trustee or administrator has not been appointed. ITSA also has responsibilities under the *Proceeds of Crime*

[115] ATO, *Annual Report 2009-10*, available at: http://www.ato.gov.au/corporate/content.aspx?menuid=49817&doc=/content/00258543.htm&page=76&H76, [accessed 8 August 2011].

Act 2002 and the *Customs Act 1901* to control and deal with property under court orders made under these statutes.[116]

ITSA is a client service organisation that collects personal information about its clients and other people such as creditors (for example names, addresses, bank account details, and income and asset information), as well as court documents relating to proceeds of crime. The agency has offices in Sydney, Melbourne, Brisbane, Adelaide, Perth, Hobart and Canberra. At 30 June 2011, ITSA employed a total of 323 full-time equivalent (FTE) employees.[117]

ITSA ICT environment

At the time of fieldwork (April – June 2011), the ITSA network did not have certification under the ISM for a specific level of classified information (See Chapter 1). However, ITSA had commissioned an ICT Security Review to assess the network infrastructure, operations and management for compliance with Australian Government requirements, identify any gaps and, where necessary, recommend a work package that would enable ITSA to achieve compliance with Australian Government standards as detailed in the PSPF, ISM and other relevant standards.

During the audit fieldwork, ITSA was also in the process of reviewing all of its ICT polices and procedures. In February 2011, ITSA established a Policy Review Group tasked with reviewing all new policy drafts and assessing them in respect of business, financial and technical aspects (including security).

[116] ITSA *Annual Report 2010-11*, Commonwealth of Australia, p. 13.

[117] ibid, p. 69.

Australian Hearing

Australian Hearing operates under the *Commonwealth Authorities and Companies Act 1997* (the CAC Act) and the *Australian Hearing Services Act 1991* (the AHS Act). Australian Hearing is part of the Human Services portfolio and reports directly to the Human Services Minister.

Australian Hearing's mission is to provide its clients with the best hearing care, the latest hearing aid technology, and to lead the world in hearing research.[118] To achieve this Australian Hearing provides hearing health services through a national network of Hearing Centres and outreach services, and undertakes research through the National Acoustic Laboratories (NAL). For this audit, the ANAO did not review the activities or work practices of the NAL, as the primary focus of the audit was on how agencies were managing the risks of PSDs that hold or transmit personal information (in Australian Hearing's case, patient-related data).

Australian Hearing provides hearing health services to Australian citizens and permanent residents through two programs:

- its Community Service Obligation (CSO) hearing services, fully funded by the government; and
- by competing with private sector companies to provide hearing services to a range of other Australians, who qualify for these services via a voucher system administered by the Office of Hearing Services in the Department of Health and Ageing.

Community Service Obligation program

Under the CSO program, Australian Hearing is funded by the Government to provide hearing services to the following groups of people[119]:

- all children and young adults up to the age of 21 (under a 2011–2012 Budget Measure this age will increase to 26 from 1 January 2012);
- Aboriginal or Torres Strait Islander people who are over 50 years of age;

[118] Australian Hearing, *Annual Report 2010*, Commonwealth of Australia, p. iii.

[119] The services are only available to people who are Australian Citizens or permanent residents.

- all participants in a Community Development Employment Projects (CDEP) Program;
- adults who qualify for a hearing services Voucher who live in remote locations not serviced by Australian Hearing's commercial competitors; and
- adults with complex hearing needs.[120]

Voucher program

In 1997 the Government introduced a voucher program for government-funded hearing services and opened the government-funded hearing services market to the private sector. Australian Hearing now competes with over 200 accredited private sector companies to provide hearing services to the following groups of people[121] who are issued with a Voucher for hearing services by the Office of Hearing Services, which is part of the Department of Health and Aged Care:

- Pensioner Concession Card Holders;
- people receiving Sickness Allowance from Centrelink;
- holders of a Gold Repatriation Health Card issued for all conditions;
- holders of a White Repatriation Health Card[122] issued for conditions that include hearing loss;
- dependents of a person in one of the above categories;
- members of the Australian Defence Force; and
- people undergoing a government-funded vocational rehabilitation service and who are referred by their service provider.

---

[120] Office of Hearing Services, <http://www.health.gov.au/internet/main/publishing.nsf/Content/health-hear-clientbudget>, [accessed 8 June 2011]. The 'adults with complex hearing needs' include those with profound hearing loss or those with hearing loss and severe communication impairment, as designated by the *Declared Hearing Services Determination 1997* (*Hearing Services Act 1991*).

[121] The services are only available to people who are Australian citizens or permanent residents.

[122] Commonwealth Gold and White Repatriation Health Cards are issued to eligible veterans of the Australian Defence Force, their widow/ers and dependents to cover the costs of all or some medical conditions. Details can be found on the Department of Veterans' Affairs internet site: < http://www.dva.gov.au/benefitsAndServices/health_cards/Pages/index.aspx>, [accessed 23 September 2011].

In 2010–11 Australian Hearing made a before-tax profit on its Voucher services of $13.8 million. Australian Hearing pays a portion of its profits each year as a dividend to the Department of Human Services. Australian Hearing employs 1 168 people nationally, with a network including a National Head Office, 111 hearing centres and over 330 outreach services.

Australian Hearing was selected for this audit as it is a client service organisation that collects personal, health-related information. As an organisation that has a large office network including mobile outreach services, it uses PSDs (particularly laptop computers) to facilitate work practices.

Australian Hearing ICT environment

Australian Hearing relies heavily on its ICT environment to facilitate its core business of providing hearing services. Australian Hearing clinicians use medical devices to perform activities such as measuring patients' hearing and adjusting hearing aids. These devices plug directly into laptop or desktop computer systems via a USB port, and software processes the information from the medical devices into a usable format (for example, a graph displaying a patient's hearing loss). The ICT systems also hold a customer management database and a clinical database, which stores patients' hearing test history.

These particular requirements mean that Australian Hearing has some constraints on its ICT environment, for example, noise sensitivities in the medical devices used by clinicians mean that only certain brands of laptop computers can be purchased for use. The use of USB ports to plug in medical devices means that some simple control mechanisms, such as physically blocking the use of USB ports, are more difficult to implement.

Information routinely stored on Australian Hearing laptops

When working away from an Australian Hearing Centre—for example, visiting a health centre in a small town or individual patients—an Australian Hearing clinician will download the agency's clinical database (called NOAH)[123] onto the local drive of their laptop computer. This enables the clinician to provide hearing services to any existing customer (for example, if someone walks into a local health centre without an appointment). The NOAH

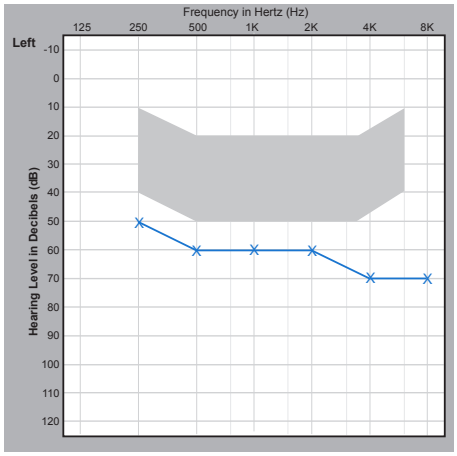
[123] NOAH is a Commercial-off-the-shelf software system designed specifically for the hearing health industry. It provides functionality for conducting hearing tests and storing the results.

database contains all customer names, an ID number which links to records in another database[124], and hearing test results.

The hearing test result information is stored as a series of numbers (frequency results) and also in graphical format. The figure below shows a typical hearing test graph stored on the NOAH database:

Figure A1

Example: Australian Hearing graph depicting a patient's hearing loss



Source: Australian Hearing.

The above graph depicts the hearing loss in a patient's left ear. The grey shaded area shows the 'normal' hearing range, and the blue line depicts the patient's degree of hearing loss across a number of frequencies.

[124] Australian Hearing has a customer service database, AHCIS, which records customer information such as appointments, contact details, hearing aid orders, and the latest hearing test. Clinicians can only access AHCIS by logging onto the Australian Hearing network, as it cannot be downloaded onto the laptop computers. Australian Hearing has developed its own software, NOAH Commander, which provides an interface between NOAH and AHCIS and allows clinicians to upload hearing test results onto the AHCIS database either via remote connection or from an Australian Hearing Centre.

Appendix 2: Sample selection methodology

As part of the audit, the ANAO undertook a survey of staff from each of the three agencies regarding the use of PSDs. The ANAO engaged ORIMA Research to assist in conducting the survey.

The ANAO selected a sample of staff from each agency to participate in the survey. The number of staff selected from each agency was determined by both the size of the agency, and an assessment of the agency's hardware and software controls. The ANAO considered the organisational impact of the survey on the two smaller agencies and selected samples representing approximately one-third of the total agency staff.

The sampling approach is outlined in Table A1.

Table A1 ANAO sampling approach

	Sample 1	Sample 2	Sample 3
Agency	ATO	Australia Hearing	ITSA
Sample Population	4660[125] Due to controls observed at the ATO, the sample population included only ATO staff with access to laptops and USB flash drives.[126]	1081[127] All Staff	442[128] All Staff
Sample	511	431	137
Number of respondents	339	241	72
Response Rates	66.3%	55.9%	52.6%

Source: ANAO.

[125] Staff list provided by the ATO.

[126] The ATO's hardware and software controls restrict the use of PSDs for ATO staff to those who have been specifically granted access.

[127] Staff list provided by Australian Hearing.

[128] Staff list provided by ITSA.

As identified above, the samples for ITSA and Australian Hearing were drawn randomly from a list of all staff provided by each agency. Given the additional controls observed at the ATO, which enforce restrictions on staff use and functionality of PSDs, the ATO sample was selected from a population of staff the ATO advised had access to corporately issued laptops and USB flash drives at the time of fieldwork. This was done to give a better representation of the ATO's use of PSDs and avoid the survey being sent to staff with little or no use of PSDs.

Appendix 3: ANAO survey findings: use of personal devices

As outlined in Chapter 4, the use of personal (that is, non-agency owned) PSDs is discouraged in advice from DSD and the Privacy Commissioner. However the ANAO survey of selected staff in each audit agency indicated that there is some use of personal devices in each agency. This is particularly the case for the use of laptop computers.

Laptop computers

Australian Taxation Office

Results of the ANAO's survey of ATO showed that of the 333 staff who answered the question regarding the use of personally owned PSDs, 82 (24.6 per cent) indicated that they had used their personally owned laptop for work purposes. Fifty-three of these staff indicated they had used their machine to store or transmit information classified as IN-CONFIDENCE or PROTECTED.

The ANAO notes that the circumstances of these cases is not known and may reflect staff using their own laptop for work-related email, or staff using their personal laptop computer to access information classified up to PROTECTED on an encrypted ATO-issued USB flash drive, which is permitted, albeit discouraged, by ATO's internal policy.

Australian Hearing

Of 239 Australia Hearing staff who answered the question regarding the use of personally owned PSDs, 42 (17.6 per cent) indicated they had used their personally owned laptop for work purposes. Fifteen of these staff indicated they had used their machine to store or transmit information classified as IN-CONFIDENCE or PROTECTED. The ANAO notes that the circumstances of these cases is not known, and that Australian Hearing does not use the PSPF information classification system.

Insolvency and Trustee Service Australia

Of 70 ITSA staff who answered the question regarding the use of personally owned PSDs, 13 (18.6 per cent) indicated they had used their personally owned laptop for work purposes. Four of these staff indicated they had used their machine to store or transmit information classified as IN-CONFIDENCE or PROTECTED.

Removable media[129]

Australian Taxation Office

Of 333 staff who answered the question regarding the use of personally owned PSDs, a number of staff indicated they had either used their personally owned removable media for work purposes, or connected them to their agency's IT network:

- USB flash drives (23);
- portable external hard drives (1); and
- CDs/DVDs (4).

The ANAO notes that the circumstances of these cases are not known and hardware and software controls observed at the ATO provide significant protection to the agency in preventing staff using personal devices.

Australian Hearing

Of the 239 staff who answered the question regarding the use of personally owned PSDs, a number of staff indicated they had either used their personally owned devices for work purposes, or connected them to their agency's IT network:

- USB flash drives (59);
- portable external hard drives (4); and
- CDs/DVDs (12).

While the use of personally owned devices is not disallowed by Australia Hearing, the survey responses also indicated 12 instances where staff had used these devices to store information classified at IN-CONFIDENCE or above.

Insolvency and Trustee Service Australia

Of staff who answered the question regarding the use of personally owned PSDs, a number indicated they had either used their personally owned devices for work purposes, or connected them to their agency's IT network:

- USB Flash drives (24);
- portable external hard drives (5); and

[129] In this audit, 'removable media' refers to USB flash drive, portable hard drives and CDs/DVDs.

- CDs/DVDs (6).

While the use of personally owned devices is not disallowed by ITSA, the survey responses also indicated nine instances where staff had used these devices to store information classified at IN-CONFIDENCE or above.

Index

Series Titles

ANAO Audit Report No.1 2011–12

The Australian Defence Force's Mechanisms for Learning from Operational Activities
Department of Defence

ANAO Audit Report No.2 2011–12
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2010 Compliance)

ANAO Audit Report No.3 2011–12
Therapeutic Goods Regulation: Complementary Medicines
Department of Health and Ageing

ANAO Audit Report No.4 2011–12
Indigenous Employment in Government Service Delivery

ANAO Audit Report No.5 2011–12
Development and Implementation of Key Performance Indicators to Support the Outcomes and Programs Framework

ANAO Audit Report No.6 2011–12
Fair Work Education and Information Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.7 2011–12
Establishment, Implementation and Administration of the Infrastructure Employment Projects Stream of the Jobs Fund
Department of Infrastructure and Transport

ANAO Audit Report No.8 2011–12
The National Blood Authority's Management of the National Blood Supply
National Blood Authority

ANAO Audit Report No.9 2011–12
Indigenous Secondary Student Accommodation Initiatives
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.10 2011–12
Administration of the National Partnership on Early Childhood Education
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.11 2011–12
Implementation and Management of the Housing Affordability Fund
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.12 2011–12
Implementation of the National Partnership Agreement on Remote Indigenous Housing in the Northern Territory
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.13 2011–12
Tasmanian Freight Equalisation Scheme
Department of Infrastructure and Transport
Department of Human Services

ANAO Audit Report No.14 2011–12
Indigenous Protected Areas
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.15 2011–12
Risk Management in the Processing of Sea and Air Cargo Imports
Australian Customs and Border Protection Service

ANAO Audit Report No.16 2011–12
The Management of Compliance in the Small to Medium Enterprises Market
Australian Taxation Office

ANAO Audit Report No.17 2011–12

Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2011

Current Better Practice Guides

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

Public Sector Audit Committees	Aug 2011
Human Resource Information Systems	
Risks and Controls	Mar 2011
Fraud Control in Australian Government Entities	Mar 2011
Strategic and Operational Management of Assets by Public Sector Entities –	
Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	Jun 2010
Planning and Approving Projects	
an Executive Perspective	Jun 2010
Innovation in the Public Sector	
Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0	
Security and Control	Jun 2009
Preparation of Financial Statements by Public Sector Entities	Jun 2009
Business Continuity Management	
Building resilience in public sector entities	Jun 2009
Developing and Managing Internal Budgets	Jun 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