



Australian Government

Office of the Privacy Commissioner

**Portable Storage Devices
and
Australian Government Agencies**

Personal Information Survey

April 2009





Australian Government

Office of the Privacy Commissioner

Portable Storage Devices and Australian Government Agencies

Personal Information Survey

April 2009



Table of Contents

1. Executive summary	5
2. Introduction	9
2.1. Background.....	9
2.2. Research objectives	10
2.3. Methodology	10
2.4. Presentation of results	11
3. Key findings	12
3.1. PSD policies	12
3.1.1. Policies about general transfers of personal information.....	12
3.1.2. Policies about agency-issued PSDs.....	15
3.1.3. Policies about private PSDs	18
3.2. Agency-issued PSDs	21
3.2.1. Provision of agency-issued PSDs	21
3.2.2. Controls on the usage of agency-issued PSDs	21
3.2.3. Training provided to staff on agency-issued PSD usage.....	25
3.2.4. Loss or theft of agency-issued PSDs	25
3.3. Private PSDs	27
3.3.1. Use of private PSDs.....	27
3.3.2. Controls on the use of private PSDs	27
3.3.3. Training provided to staff on private PSD usage	30
3.3.4. Loss or theft of private PSDs.....	30

Appendices

Appendix A: Glossary of Terms.....	33
Appendix B: Questionnaire.....	37
Appendix C: List of Agencies that Completed the Survey.....	63



1. Executive summary

Background

During March - April 2009 the Office of the Privacy Commissioner (the Office) conducted a benchmark online survey of Australian Government agencies to identify how they have addressed the risks Portable Storage Devices¹ (PSDs) present to their management of personal information in the workplace.

The survey fieldwork was undertaken by Orima Research Pty Ltd on behalf of the Office, and the data were collected between 10 March and 6 April 2009.

The survey received a very positive response from agencies, with a total of 94 survey returns received out of 118 agencies that were sent survey invitations, representing a response rate of 80%.

The survey was undertaken in the context of the increasing use of PSDs in Australia and reports of large scale breaches overseas involving loss of laptops, CDs and USB keys.

Survey Findings

The survey found that most agencies have a range of policies in place governing the transfer of personal information and usage of PSDs. Agencies were much more likely to have policies about general transfers of personal information and the usage of agency-issued PSDs than they were to have policies about the usage of private PSDs.

There were mixed results regarding the extent of controls around the use of agency-issued PSDs and private PSDs. It was common for agencies to maintain a register of agency-issued PSDs and undertake an annual stocktake. Most agencies prohibited at least some private PSDs from the workplace and just over half implemented software controls on private PSD usage. Controls on the usage of agency-issued PSDs and private PSDs were more common amongst larger agencies than smaller agencies.

Over half of agencies indicated that they had experienced the loss or theft of an agency-issued PSD in the previous 12 months, while under one-fifth indicated that they were aware of the loss or theft of a private PSD that had been used to store personal information held by their agency.

¹ See glossary in Appendix A for a definition of PSDs.

PSD Policies

While a high proportion of agencies had policies in place around the transfer of personal information and the use of agency-issued PSDs, a much lower share of agencies had policies in place about the use of private PSDs by their staff.

- ◆ Around three-quarters of agencies indicated that they had policies in place to address the secure transfer of records containing personal information:
 - within their agency (77%);
 - outside their agency (75%); and
 - for staff temporarily working away from their office (69% as a dedicated policy and 6% as part of more general guidelines).
- ◆ Around 80% of agencies had policies in place to govern the use of agency-issued PSDs (81%) and for reporting the loss or theft of an agency-issued PSD (80%).
- ◆ Just over half of agencies (55%) had specific policies in place to govern the use of private PSDs.
 - The likelihood of agencies having these policies increased with agency size – 26% of very small agencies², 48% of small agencies, 54% of medium agencies and 81% of large agencies.
- ◆ 27% of agencies had documented policies for reporting the loss or theft of a private PSD that may have been used to store personal information belonging to the agency.
 - These policies were also more prevalent amongst larger agencies – ranging from 8% of very small agencies to 41% of large agencies.

Agency-Issued PSDs

All agencies indicated that they provide access to PSDs to their staff.

- ◆ Laptops/notebooks were issued by all agencies and over three-quarters of agencies issued a range of other devices including mobile phones/mp3 players/iPods (91%), USB/portable flash memory (91%), CDs/DVDs (80%) and PDAs (79%).

While the vast majority of agencies maintain a register of their agency-issued PSDs (97%) and undertake an annual stocktake (85% of those with a register), low to moderate proportions provide a range of other controls.

² 'Very small agencies' are defined as having less than 100 staff, 'small agencies' have 100 to 250 staff, 'medium agencies' have 251 to 1000 staff and 'large agencies' have more than 1000 staff.

- ◆ Less than two-thirds of agencies classify their agency-issued PSDs in line with their Information Classification Scheme (e.g. the Protective Security Manual (PSM)³) (62%).
- ◆ Just over half of agencies (56%) indicated that their agency-issued PSDs are required to have a minimum standard of encryption.
 - Encryption was most commonly applied to laptops/notebooks (48% of agencies that issued them) and PDAs (45%).
- ◆ Under one-third (30%) of agencies indicated that they can identify whether files or other data have been transferred to an agency-issued PSD (with most of these agencies only being able to identify transfers to some PSDs).
 - This capability was greater amongst large agencies (46%), than medium (33%), small (14%) or very small (21%) agencies.

Less than two-thirds of agencies indicated that they provide staff with training on the use of agency-issued PSDs and relevant security requirements (63%).

Over half (58%) of agencies indicated that they experienced the loss or theft of an agency-issued PSD in the previous 12 months.

- ◆ 96% of large agencies experienced the loss or theft of an agency-issued PSD over this period, compared with 54% of medium agencies, 52% of small agencies and 15% of very small agencies.

1.1. Private PSDs

Around three-quarters of agencies permit the use of at least some private PSDs in the workplace.

- ◆ 40% of agencies permit the use of *all* PSDs.
 - Large agencies were the least likely to permit all private PSDs (25%), followed by medium agencies (38%), small agencies (43%) and very small agencies (60%).
- ◆ 37% of agencies permit the use of *some* private PSDs. The most common type of private PSD *prohibited* by these agencies is laptops/notebooks.

While just over half of agencies implement software controls⁴ on the use of private PSDs, other controls on private PSDs are implemented by under one-quarter of agencies.

³ The PSM requires that, if information is security classified, then any media or device storing that information must be classified to at least the same level.

⁴ See glossary in Appendix A for a definition of software controls.

- ◆ 54% of agencies indicated that they use software controls (most commonly operating system controls) to restrict or control the use of private PSDs.
- ◆ 20% of agencies indicated that they could identify whether files or data have been transferred to a private PSD.
 - This capability was greater amongst large agencies (36%), than medium (21%), small or very small agencies (both 10%).
- ◆ 16%⁵ of agencies indicated that they use hardware controls⁶ (most commonly disabling USB ports) to restrict or control the use of private PSDs.

Around one-quarter of agencies that allow private PSD usage indicated that they provide staff with training on the use of private PSDs in the workplace and relevant security requirements (24%).

- ◆ 44% of agencies with at least one office outside Australia indicated that they provided staff with training, compared with 20% of agencies with no offices outside Australia.

Less than one-fifth of agencies (18%) indicated that they had experienced the loss or theft of privately owned PSDs that had been used to store personal information held by the Agency in the previous 12 months.

- ◆ Large agencies (44%) and agencies engaging more than 50 Contracted Service Provider (CSP⁷) staff (55%) experienced the highest incidence of loss or theft of private PSDs.

⁵ Agencies that did not answer this question but that indicated that they allow PSDs to be used in the workplace were interpreted as having no hardware controls.

⁶ See glossary in Appendix A for a definition of hardware controls.

⁷ See glossary in Appendix A for a definition of CSP.



2. Introduction

2.1. Background

Portable Storage Devices (PSDs) are small, lightweight, portable, easy to use electronic devices, which are capable of storing and transferring large volumes of data.

A PSD may be either exclusively used for data storage (e.g. portable external hard drives, CDs/DVDs, USB keys) or may be capable of a range of other functions (e.g. laptops/ notebooks, personal digital assistants (PDAs) such as Pocket PC, Palm, BlackBerry, and devices with in-built accessible storage such as MP3 players, iPods, and mobile phones).

In general terms, PSDs provide a number of advantages for users – they enable large amounts of information to be transferred swiftly, and provide increased convenience and portability in the storage of this information and data. They are widely available, relatively inexpensive and generally very simple to use.

These advantages, however, pose specific challenges for Australian Government agencies, especially around maintaining appropriate storage and security of personal information held by the agency as required by Information Privacy Principle (IPP) 4 of the *Privacy Act 1988 (Cth)* (the Act).

These obligations require agencies to maintain security safeguards that are reasonable in the circumstances to protect the personal information⁸ they hold from loss, unauthorised access, use, modification, disclosure and against other misuses.

The *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009* (PSD survey) was undertaken to assess how Australian Government agencies are currently addressing the risks that both agency-issued and privately owned PSDs present to their management of personal information in the workplace.

⁸ 'Personal information' is defined in Section 6 of the Act 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'.



2.2. Research objectives

The main objectives of the survey were to:

- ◆ identify privacy controls that govern how personal information is transferred both within and between Australian Government agencies, and external organisations
- ◆ identify the current privacy controls that Australian Government agencies have in place around the use of PSDs, both those issued by an agency to staff and those privately owned by staff
- ◆ identify good privacy practices and policies
- ◆ identify any areas of concern that may need to be addressed across Australian Government agencies and
- ◆ inform the development of future guidance material by the Office to assist Australian Government agencies to maintain appropriate policies and procedures to minimise the risks presented by the use of PSDs.

The survey will also provide a benchmark measure against which the future performance of Australian Government agencies' use of PSDs and their personal information handling practices may be compared.

2.3. Methodology

The data collection method for the survey was an online questionnaire.

The survey questionnaire was designed by the Office, and was based on a similar survey undertaken in 2008 by the Office of the Victorian Privacy Commissioner which covered Victorian public sector agencies⁹.

The survey fieldwork, data analysis and reporting were undertaken by ORIMA Research Pty Ltd (ORIMA) on behalf of the Office.

In February 2009, a letter was sent by the Australian Privacy Commissioner to the heads of Australian Government agencies advising them of the proposed survey and

⁹ A copy of this report, *Use of Portable Storage Devices*, is available from the Office of the Victorian Privacy Commissioner's website at <http://www.privacy.vic.gov.au/>

inviting each agency to participate in the research. The relevant Privacy Contact Officer (PCO) for each agency was identified as the most appropriate primary point of contact for the survey, although agencies were able to nominate an alternative contact if appropriate. If an agency did not have a PCO, the agency was asked to nominate an appropriate individual as the primary point of contact for the survey.

An invitation email containing details of the survey was then sent to all nominated contact officers on 10 March 2009. Completed survey responses were accepted from agencies up until 6 April 2009.

The questionnaire contained 99 questions, the majority of which involved a forced choice. Several open-ended questions were also provided for respondents to comment on specific issues.

A total of 94 out of 118 Australian Government agencies that were 'in-scope' for the survey completed the questionnaire, representing an overall response rate of 80%.

2.4. Presentation of results

Percentages shown in this report are based on the total number of valid responses made to the particular question being reported on.

In most cases, results reflect those agencies that expressed a view and to which the questions were applicable. 'Not applicable' / 'don't know' responses have only been presented where this significantly aids in the interpretation of the results.

Percentage results throughout the report may not add up to 100% due to rounding, or due to questions that allow respondents to give more than one answer.

3. Key findings

The *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009* found that most agencies have a range of policies in place governing transfers of personal information and usage of PSDs.

Agencies were much more likely to have policies about general transfers of personal information and the usage of agency-issued PSDs than they were to have policies about the usage of private PSDs. The proportion of agencies that had policies in place governing the transfer of personal information and usage of PSDs was also much higher amongst larger agencies than smaller agencies.

There were mixed results regarding the extent of controls around the use of agency-issued PSDs and private PSDs. It was common for agencies to maintain a register of agency-issued PSDs and undertake an annual stocktake, however, few agencies labelled agency-issued PSDs regarding unauthorised use and return and there was limited capability to detect transfers of files or data to agency-issued PSDs.

Most agencies prohibited at least some private PSDs from the workplace and just over half implemented software controls on private PSD usage. Hardware controls on private PSD usage were, however, rare and few agencies could detect when files or data had been transferred to private PSDs. Controls on the usage of agency-issued PSDs and private PSDs were more common amongst larger agencies than smaller agencies.

Over half of agencies indicated that they had experienced the loss or theft of an agency-issued PSD in the previous 12 months, while under one-fifth indicated that they were aware of the loss or theft of a private PSD that had been used to store personal information held by their agency. The lower awareness of the loss or theft of private PSDs may partly reflect the fact that many agencies had no policy in place or other process to detect when these losses or thefts occurred.

3.1. PSD policies

While a high proportion of agencies indicated that they had policies in place surrounding the transfer of personal information and usage of agency-issued PSDs, a much lower share indicated that they had policies in place about the use of private PSDs by their staff.

3.1.1. Policies about general transfers of personal information

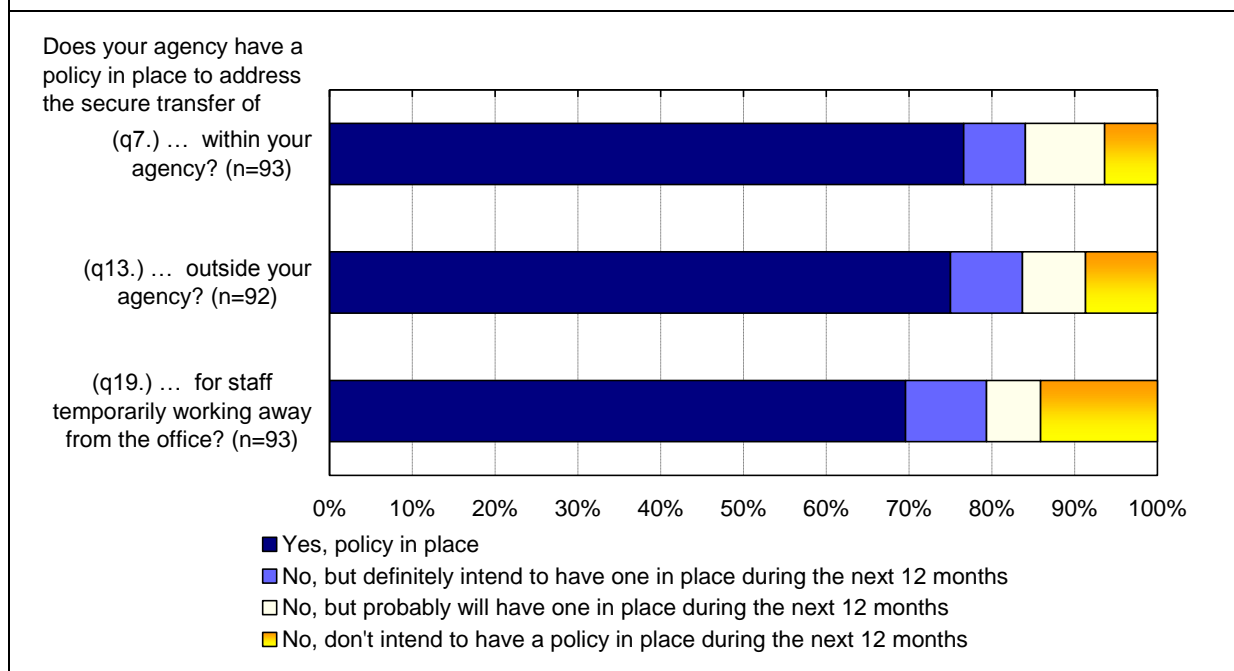
Figure 1 shows that policies about the general transfer of personal information were in place in over two-thirds of agencies that took part in the survey.

- ◆ Around three-quarters of agencies indicated that they had policies in place to address the secure transfer of records containing personal information within (77%) and outside (75%) their agency.
 - At least 90% of agencies with these policies in place indicated that the policies covered both physical and electronic records.
 - Around one-third of agencies that did not currently have these policies in place 'definitely' intended to develop them in the next 12 months (32% for policies about transfers within agencies and 35% for outside agencies), while a broadly similar share 'probably' intended to develop them over this period (41% and 30% respectively).
 - The most common single reason (identified by about one-third of relevant agencies) cited by those agencies that did not have such policies in place nor intended to develop them in the next 12 months was that they felt the lack of such a policy was low risk for their agency.
- ◆ Agencies were slightly less likely to have policies in place to address the secure transfer of personal information for staff temporarily working away from the office (69%, although a further 6% of agencies indicated that this was addressed by more general guidelines).
 - At least 90% of agencies with policies in place about transfers of personal information for staff working away from the office indicated that these policies covered both physical (91%) and electronic (97%) records.
 - 32% of agencies that did not currently have these policies in place 'definitely' intended to develop them in the next 12 months, while 21% 'probably' intended to develop them over this period.
 - 29% of agencies that did not have such policies in place nor intended to develop them in the next 12 months indicated that this was because the lack of such a policy was low risk for their agency.



Figure 1: Policies about general transfers of personal information

(% of agencies)



Policies about general transfers of personal information by agency size

There was considerable variation in the likelihood of having policies in place to address the transfer of personal information based on agency size. Figure 2 shows that:

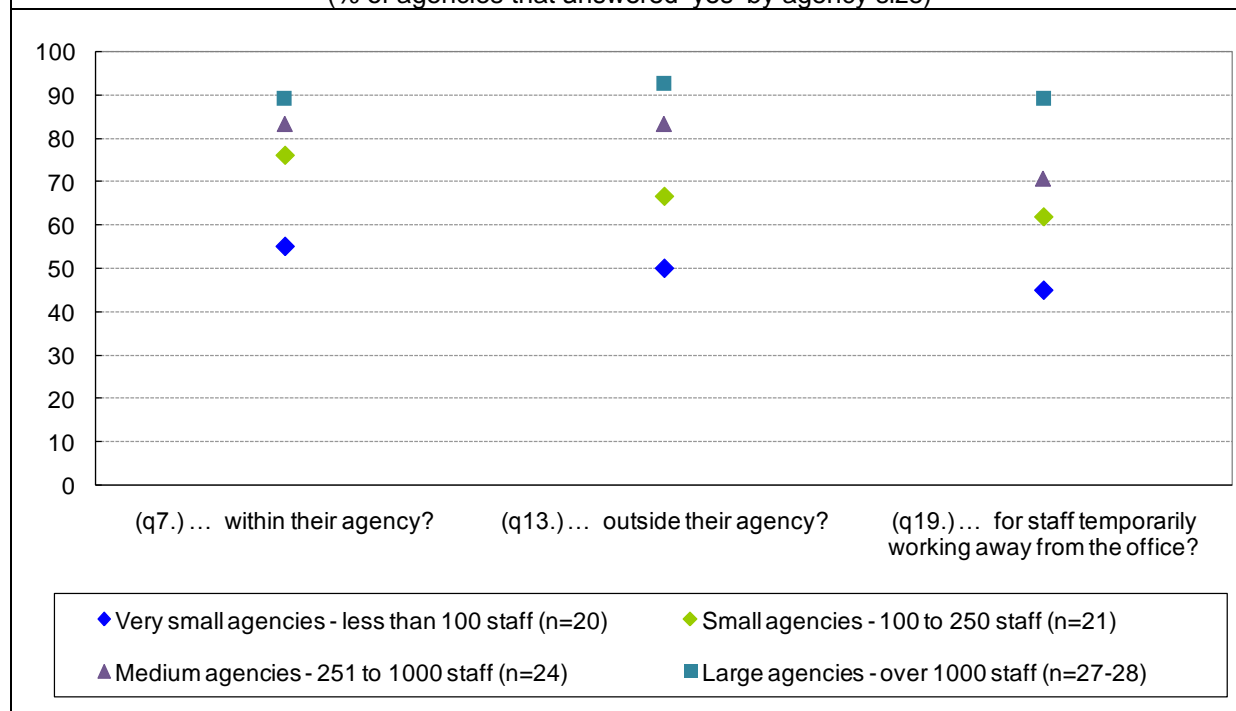
- ◆ 89% of large agencies had policies for transfers of information *within* their agency, compared with 55% of very small agencies;
- ◆ 93% of large agencies had policies in place for transfers of information *outside* their agency, compared with 50% of very small agencies; and
- ◆ 89% of large agencies had policies in place to address the secure transfer of records for staff working away from the office, compared with 45% of very small agencies.

Small agencies that had policies in place about general transfers of personal information were less likely than agencies of other sizes to have policies covering electronic records:

- ◆ within their agency (81%, compared with between 91% and 100% of other agencies);
- ◆ outside their agency (71%, compared with between 90% and 100% of other agencies); and
- ◆ for staff temporarily working away from the office (85%, compared with 100% of other agencies).

Figure 2: The extent to which agencies had policies in place to address the secure transfer of records containing personal information ...

(% of agencies that answered 'yes' by agency size)



3.1.2. Policies about agency-issued PSDs

Figure 3 shows that around 80% of agencies had various policies in place about the use, loss/theft and disposal of agency-issued PSDs.

- ◆ 81% of agencies had specific policies in place to govern the use of agency-issued PSDs.
 - Of those agencies with policies in place, 59% indicated that their policies covered all types of PSDs while the remainder indicated that their policies covered¹⁰:
 - laptops/notebooks (33%);
 - PDAs (29%);
 - Mobile phones/MP3 players/iPods (28%); and
 - USB/portable flash memory (21%).

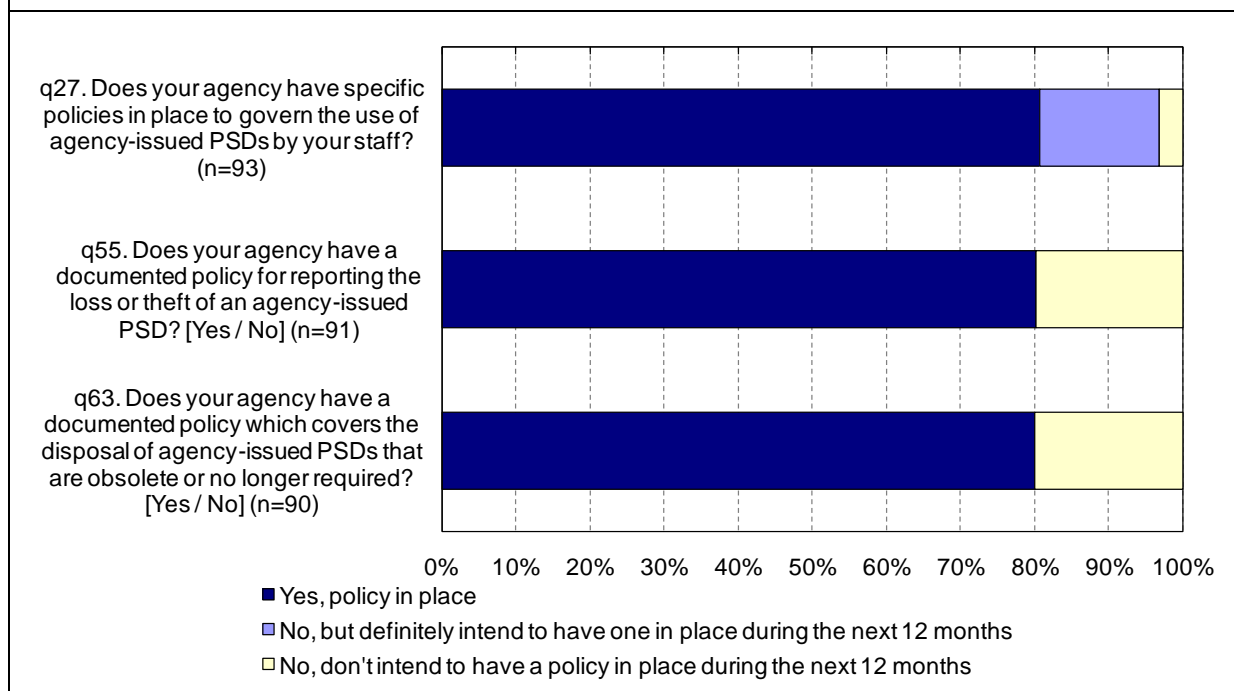
¹⁰ Multiple responses were permitted for this question, so percentage results will not add to 100%.

- Around half of agencies with these policies in place (47%) indicated that the policy prescribed how agency data containing personal information is to be deleted from PSDs.
- Agencies that had these policies in place most commonly made staff aware of them by placing the policies on their intranet (91%), via induction training (62%) and by making it the responsibility of staff (62%) or their managers (41%) to raise awareness.
- 83% of agencies that did not currently have policies about agency-issued PSDs in place intended to develop them in the next 12 months.
- ◆ 80% of agencies indicated that they had policies in place for reporting the loss or theft of an agency-issued PSD.
 - Of those agencies with policies in place, 28% had a specific policy or incident reporting policy covering agency-issued PSDs, while the remainder covered them as part of their general loss / incident reporting policy.
 - 57% of agencies that had specific policies in place indicated that they covered all PSDs, and over one-quarter indicated that they covered PDAs (30%), laptops/notebooks (26%) and mobile phones/MP3 players/iPods (26%).
 - Those agencies that did not have a policy in place for reporting the loss or theft of agency-issued PSDs indicated that they generally identified when an agency-issued PSD had been lost or stolen by being advised by the staff member to whom the PSD had been issued. A few agencies also indicated that they identified these losses and thefts through regular stocktakes or audits.
- ◆ 80% of agencies had a policy in place which covers the disposal of agency-issued PSDs that are obsolete or no longer required.
 - Of those agencies with policies in place, 18% had a specific PSD disposal policy, which generally applied to all PSDs (77%).



Figure 3: Policies about agency-issued PSDs

(% of agencies)



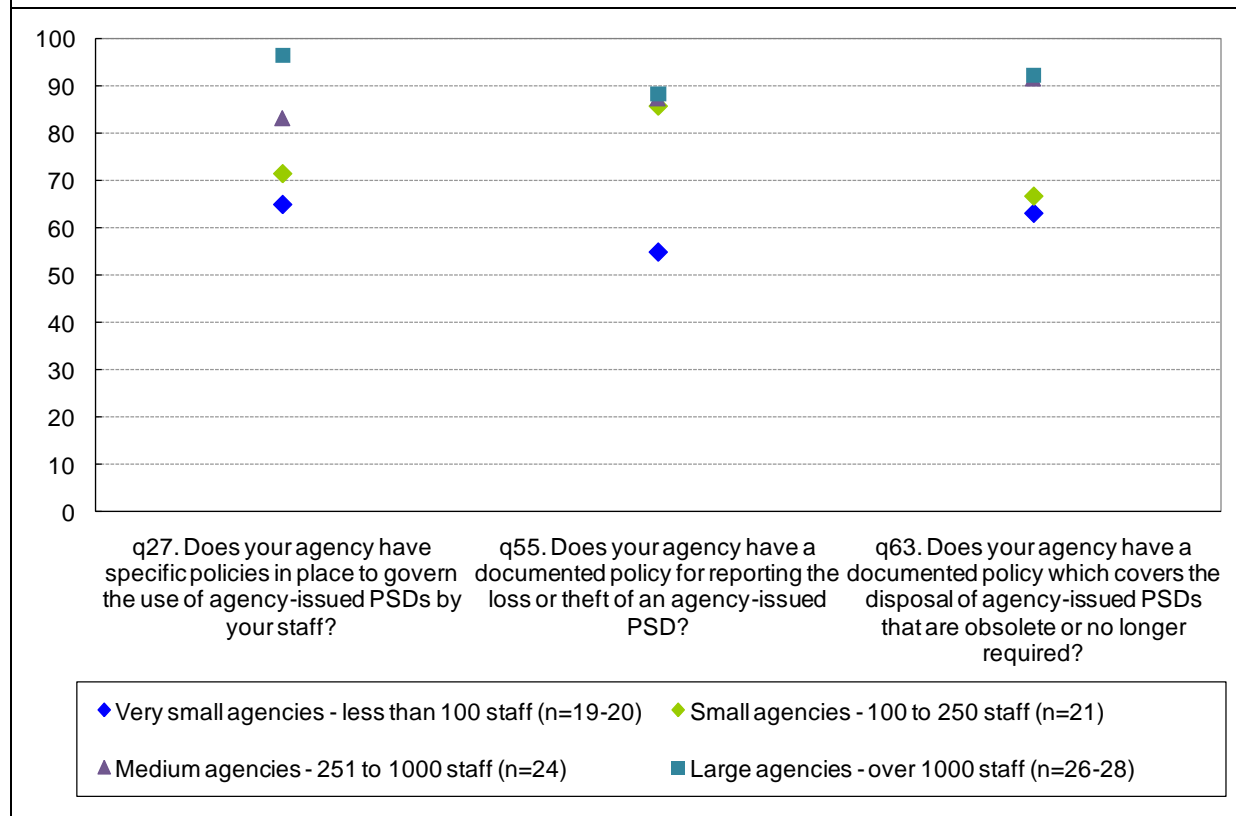
Policies about agency-issued PSDs by agency size

Those agencies with less than 100 staff (i.e. very small agencies) were the least likely to have policies in place regarding agency-issued PSDs. Figure 4 shows that:

- ◆ the likelihood of having specific policies in place to govern the use of agency-issued PSDs ranged from 65% for very small agencies to 96% for large agencies;
- ◆ just over half of very small sized agencies (55%) had a loss or theft policy in place for agency-issued PSDs, well below the share of larger-sized agencies (86% to 88%); and
- ◆ around two-thirds of very small (63%) and small (67%) agencies had policies in place about the disposal of obsolete agency-issued PSDs, compared with 92% of both medium and large agencies.

Figure 4: Policies about agency-issued PSDs by agency size

(% of agencies that answered 'yes' by agency size)

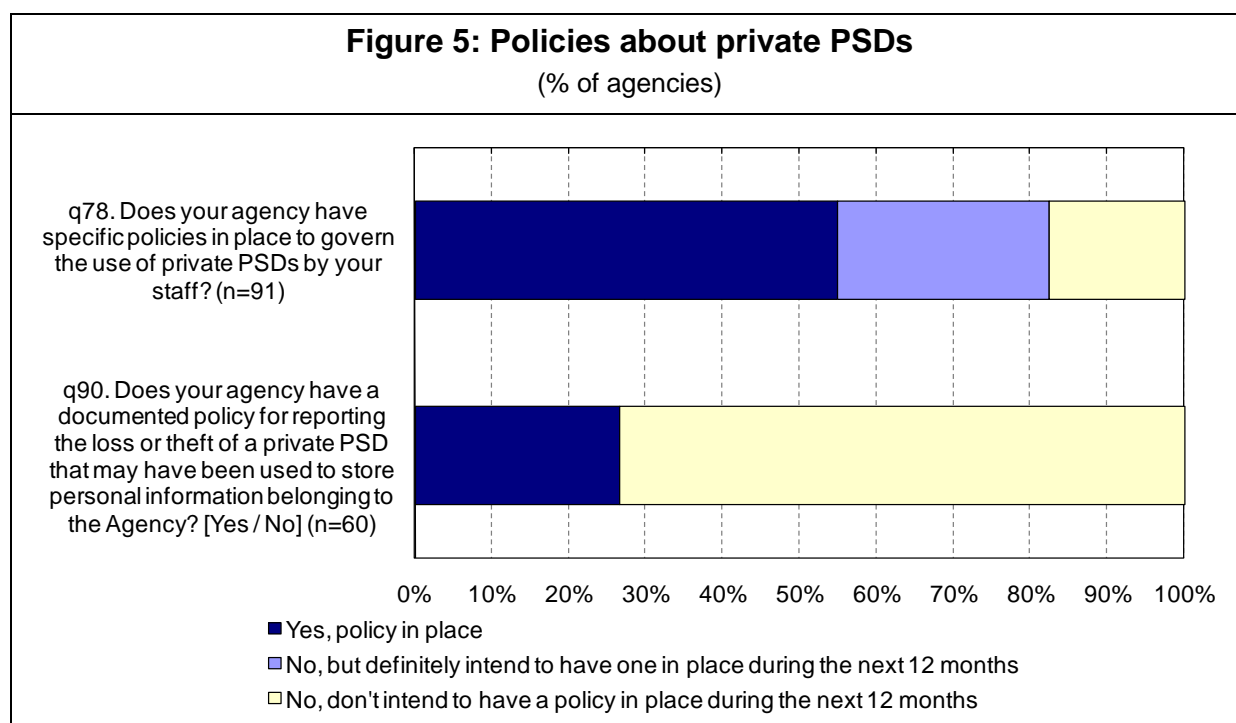


3.1.3. Policies about private PSDs

Agencies were much less likely to have policies in place about the use of private PSDs by their staff than the use of agency-issued PSDs.

- ◆ Figure 5 shows that just over half (55%) of agencies indicated that they have specific policies in place to govern the use of private PSDs. The vast majority of these policies (82%) applied to all PSDs.
 - 45% of agencies that had these policies in place indicated that the policies prescribed how agency data containing personal information stored on a private PSD is to be deleted.
 - Agencies that had these policies in place most commonly made staff aware of them by placing the policies on their intranet (92%), via induction training (71%) and by making it the responsibility of staff (e.g. by signing an Acceptable Use agreement) (61%) or their managers (45%) to raise awareness.
 - 61% of agencies that did not currently have these policies in place intended to develop them in the next 12 months.

- 50% of agencies that did not have such policies in place nor intended to develop them in the next 12 months indicated that this was because the lack of such a policy was low risk for their agency.
- ◆ This figure also shows that around one-quarter (27%) of agencies indicated that they have documented policies for reporting the loss or theft of a private PSD that may have been used to store personal information belonging to the agency. The vast majority of these policies (81%) applied to all PSDs.
 - Of those agencies with such policies, only two (13%) had a *specific* policy for reporting the loss or theft of a private PSD.
 - Those agencies that did not have such policies generally indicated that they did not find out about the loss or theft of private PSDs, or were reliant on the user to report it.



Policies about private PSDs by agency size

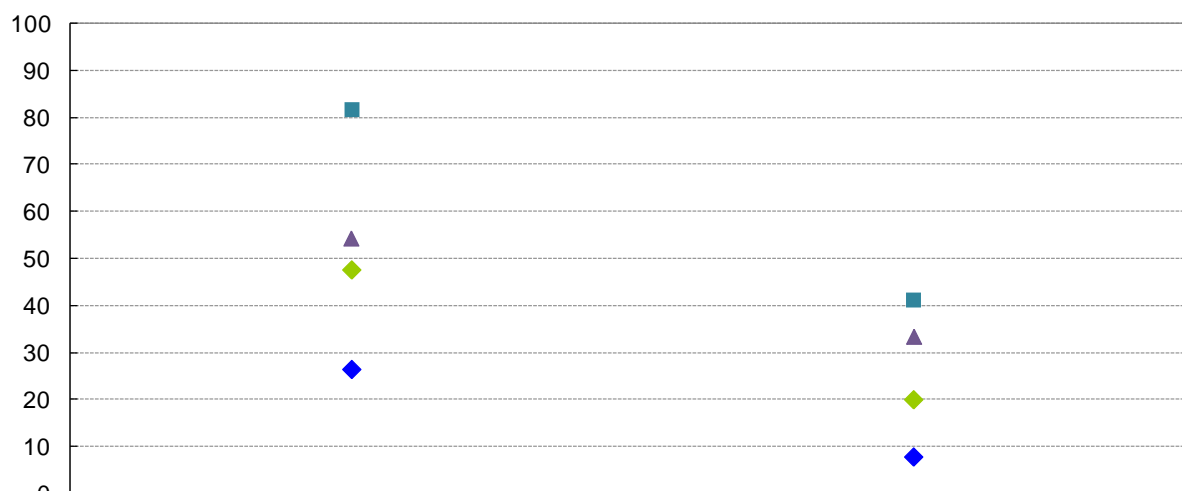
Very small agencies were the least likely to have policies in place about private PSDs. Figure 6 shows that:

- ◆ the likelihood of agencies having policies in place to govern the use of private PSDs increased strongly with the size of the agency – 26% of very small agencies, 48% of small agencies, 54% of medium agencies and 81% of large agencies; and
- ◆ the likelihood of agencies having policies in place for reporting the loss or theft of a private PSD also increased with the size of the agency – 8% of very small

agencies, 20% of small agencies, 33% of medium agencies and 41% of large agencies.

Figure 6: Policies about private PSDs by agency size

(% of agencies that answered 'yes' by agency size)



q78. Does your agency have specific policies in place to govern the use of private PSDs by your staff?

q90. Does your agency have a documented policy for reporting the loss or theft of a private PSD that may have been used to store personal information belonging to the Agency?

- ◆ Very small agencies - less than 100 staff (n=13-19)
- ◆ Small agencies - 100 to 250 staff (n=15-21)
- ▲ Medium agencies - 251 to 1000 staff (n=15-24)
- Large agencies - over 1000 staff (n=17-27)



3.2. Agency-issued PSDs

3.2.1. Provision of agency-issued PSDs

All agencies indicated that they provide staff with agency-issued PSDs and 36% of agencies indicated that they provide access to agency-issued PSDs to Contracted Service Providers (CSPs). The most common types of PSDs provided by agencies included:

- ◆ laptops/notebooks – provided by 100% of agencies;
- ◆ mobile phones/mp3 players/iPods (91%);
- ◆ USB/Portable Flash memory (91%);
- ◆ CDs/DVDs (80%); and
- ◆ PDAs (79%).

3.2.2. Controls on the usage of agency-issued PSDs

Figure 7 shows that some controls on the usage of agency-issued PSDs were used by almost all agencies, however, others were used by well under half of agencies.

- ◆ Almost all agencies kept a register of agency-issued PSDs (97%) and the vast majority undertook an annual stocktake of agency-issued PSDs (85% of agencies that keep a register).
 - Only 27% of agencies that maintain registers indicated that the registers covered all PSDs, with registers most commonly covering laptops/notebooks (72%), mobile phones/MP3s/iPods (65%) and PDAs (56%).
 - The coverage of stocktakes closely mirrored the composition of registers in most agencies. Across all agencies that keep a register of PSDs, at least 70% undertook stocktakes on the devices on their register.
 - The small minority of agencies that maintained a register but did not undertake an annual stocktake (thirteen agencies or 15%), most commonly indicated that this was because:
 - they considered that not undertaking a stocktake was low risk to their agency (42%);
 - the items on the register were low cost (33%); and/or
 - it was felt to be cost prohibitive to conduct a stocktake (25%).



- ◆ Almost two thirds of agencies required staff to sign an agreement with the agency around their acceptance of the terms and conditions of use of agency-issued PSDs (63%) and classify their agency-issued PSDs in line with their Information Classification Scheme (e.g. the Protective Security Manual (PSM)¹¹) (62%).
 - Of those agencies that require staff to sign an agreement to use agency-issued PSDs, 30% required this for all PSDs, while over 40% required this for laptops/notebooks (61%), mobile phones/MP3s/iPods (46%) and PDAs (42%).
 - Three-quarters of agencies (75%) that require staff to sign an agreement to use agency-issued PSDs indicated that these agreements specify that the staff member agrees to adhere to relevant agency and Australian Government policies and procedures¹².
- ◆ Just over half of agencies (56%) indicated that agency-issued PSDs are required to have a minimum standard of encryption.
 - Encryption was most commonly applied to laptops/notebooks (48% of agencies that issued them) and PDAs (45%), followed by portable hard drives and USB/Portable flash memory (both 25%). It was uncommon for agencies to apply encryption to mobile phones/MP3s/iPods (8%) and CDs/DVDs (4%).
 - 28% of agencies that indicated that they require a minimum standard of encryption for agency-issued PSDs indicated that this was provided by their agency, 18% indicated that it was supplied with the device (i.e. native encryption) and 54% indicated it was both provided by their agency and supplied with the device.
- ◆ Under one third (30%) of agencies indicated that they can identify whether files or other data have been transferred to an agency-issued PSD (with most of these agencies only being able to identify transfers from *some* PSDs).
- ◆ Only one quarter or less of agencies indicated that they label agency-issued PSDs regarding unauthorised use and return.
 - 25% of agencies indicated that agency-issued PSDs are labelled clearly with a warning against unauthorised use.
 - No agencies that labelled their agency-issued PSDs against unauthorized use indicated that this was applied to all PSDs. These agencies indicated that it was most commonly applied to laptops/notebooks (91%), PDAs (41% of agencies that issued PDAs) and portable hard drives (33% of agencies that issued hard drives).

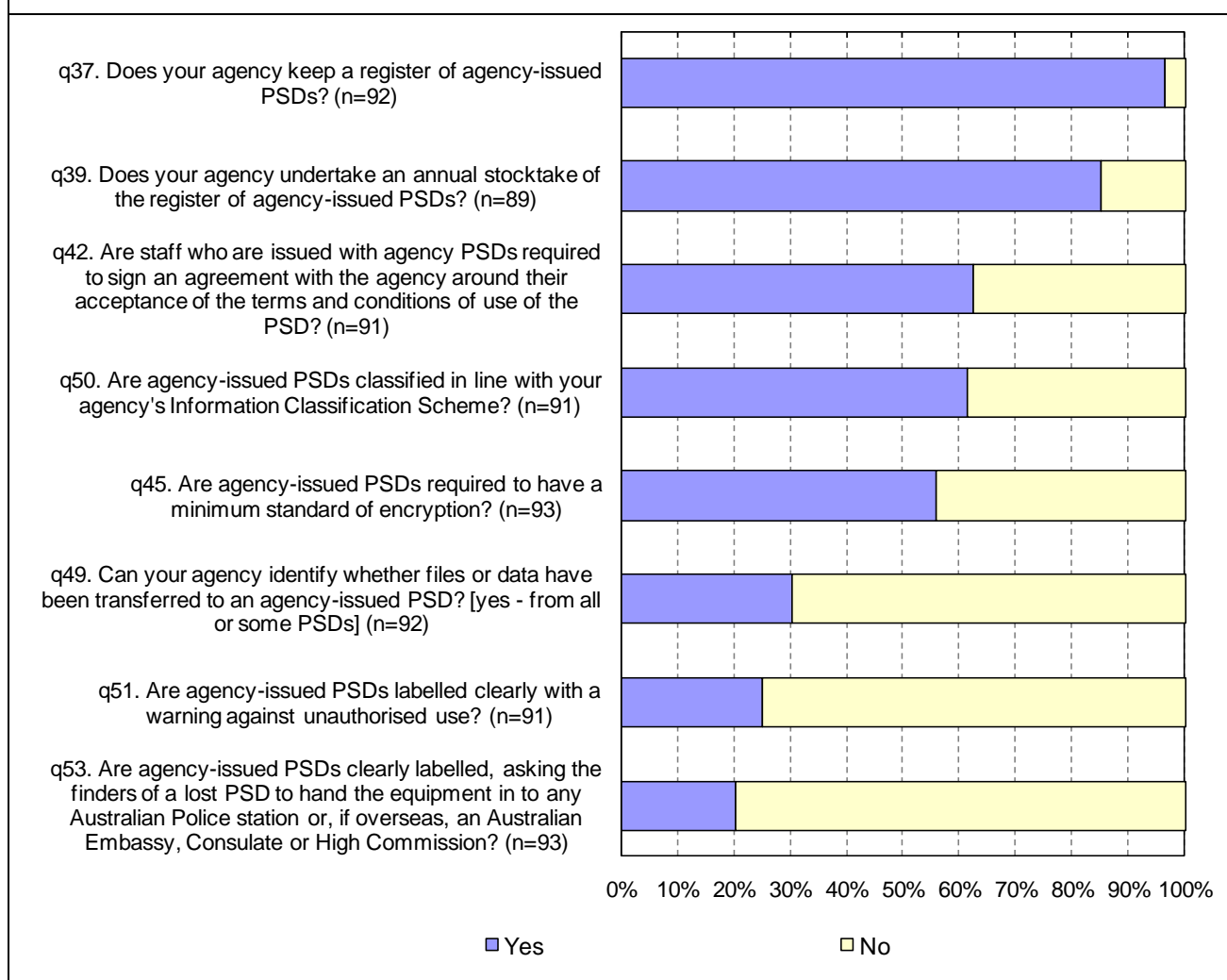
¹¹ The PSM requires that, if information is security classified, then any media or device storing that information must be classified to at least the same level.

¹² Relevant agency and Australian Government policies and procedures include the Protective Security Manual, Chief Executive Guidance and the *Australian Government ICT Security Manual* (ACSI 33).

- 20% of agencies indicated that PSDs are clearly labelled, asking finders of a PSD to hand the equipment in to relevant agencies.
 - No agencies that labelled their agency-issued PSDs asking finders to hand them into the relevant agencies indicated that this was applied to all PSDs. These agencies indicated that it was most commonly applied to laptops/notebooks (61%), PDAs (54% of agencies that issued PDAs) and mobile phones/MP3s/iPods (25% of agencies that issued mobile phones/MP3s/iPods).

Figure 7: Extent to which agencies have controls on the usage of agency-issued PSDs

(% of agencies)



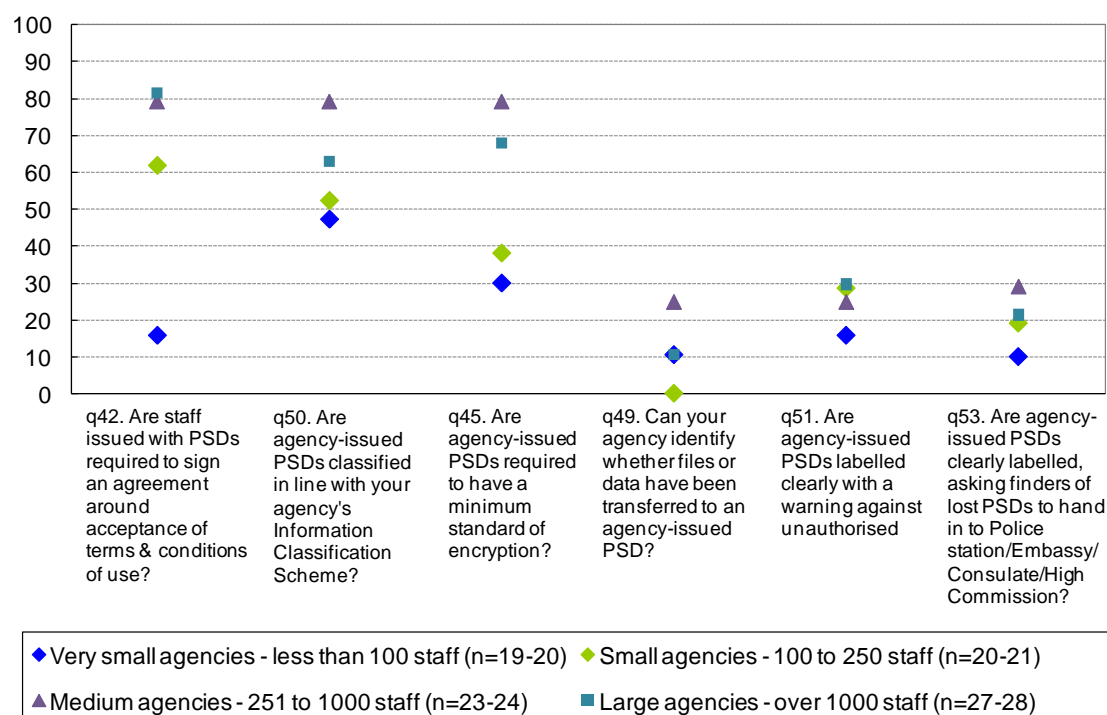
Controls on the usage of agency-issued PSDs by agency size

While almost all agencies, irrespective of size, maintained a register and undertook an annual stocktake of agency-issued PSDs, the survey showed that there was considerable variation in the extent to which agencies implemented other controls on the usage of these PSDs by agency size. Large agencies were significantly more likely to use several of these controls than smaller agencies. Figure 8 shows that:

- ◆ only 16% of very small sized agencies require staff to sign an agreement around the acceptable use of agency-issued PSDs, compared with between 62% and 81% of larger sized agencies;
- ◆ 79% of medium-sized agencies indicated that their agency-issued PSDs are classified in line with their Information Classification Scheme (e.g. PSM), compared with between 47% and 63% of other sized agencies;
- ◆ well over half of medium (79%) and large (69%) agencies required a minimum standard of encryption for agency-issued PSDs, compared with well under half of small (38%) and very small (30%) agencies; and
- ◆ almost half (46%) of large agencies were able to identify whether data or files had been transferred to agency-issued PSDs, compared with one-third (33%) of medium agencies, and less than one-quarter of small (14%) or very small agencies (21%).

Figure 8: Extent to which agencies have controls on the usage of agency-issued PSDs

(% of agencies that answered 'yes' by agency size)



3.2.3. Training provided to staff on agency-issued PSD usage

Less than two-thirds of agencies indicated that they provided staff with training on the use of agency-issued PSDs and relevant security requirement (63%), with the most common delivery method being on-the-job training (67%).

- ◆ Agencies with at least one office outside Australia (71%) were more likely to provide staff with training, compared with agencies with no offices outside Australia (62%).
- ◆ 88% of medium-sized agencies provided staff with training on the use of agency-issued PSDs, compared with between 40% and 67% of other sized agencies.

3.2.4. Loss or theft of agency-issued PSDs

Over half of agencies (58%) indicated that they experienced the loss or theft of an agency-issued PSD¹³ during the previous 12 months.

- ◆ 89% of these agencies were able to estimate the number of agency-issued PSDs lost or stolen over this period. The most common number of agency-issued PSDs lost or stolen was between 2 and 10 PSDs (58%), however, 16% of agencies lost 10 or more.
 - The maximum estimated number of agency-issued PSDs lost or stolen from a single agency over this period was 200¹⁴.
 - 91% of agencies that had an agency-issued PSD lost or stolen over this period that stored personal information held by the agency found out about this by being notified by staff.

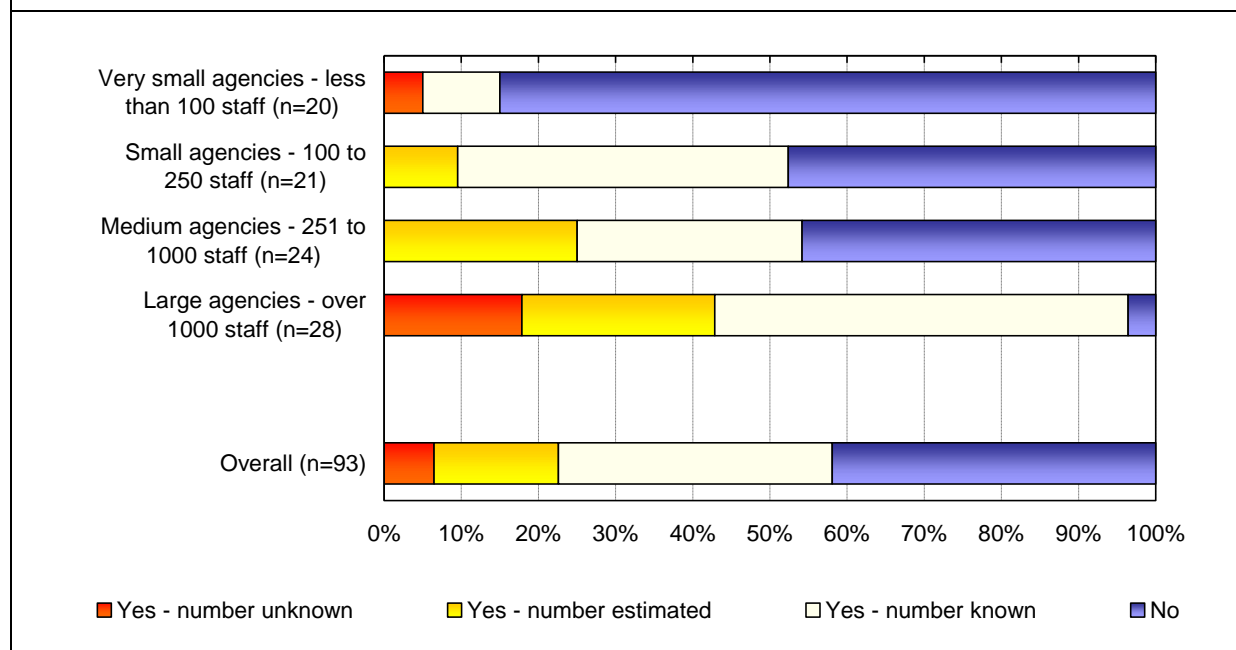
Large agencies and agencies engaging more than 50 CSP staff experienced the highest incidence of loss or theft of agency-issued PSDs.

- ◆ Figure 9 shows that 96% of large agencies experienced the loss or theft of an agency-issued PSD, compared with 54% of medium agencies, 52% of small agencies and 15% of very small agencies.
- ◆ 100% of agencies that engage more than 50 CSP staff experienced the loss or theft of an agency-issued PSD.

¹³ This result is for all PSDs lost or stolen during the previous 12 months, not just for those that were lost or stolen that had been used to store personal information held by the agency.

¹⁴ This was one of the largest agencies that completed the survey. The agency's response indicated that it employed over 5,000 staff and issued a range of PSDs to both agency and CSP staff, including laptops/notebooks, CDs/DVDs, PDAs and mobile phones/MP3s/iPods.

Figure 9: Loss or theft of agency-issued PSDs by agency size
(% of agencies)



3.3. Private PSDs

3.3.1. Use of private PSDs

Around three quarters of agencies allow at least some private PSDs to be used in the workplace.

- ◆ Just under one-quarter of agencies prohibit all types of private PSDs in the workplace (24%).
- ◆ Just under two-fifths (37%) of agencies prohibit some types of private PSDs in the workplace.
 - The most common private PSDs prohibited by these agencies are laptops/notebooks (78%), while around two-fifths of these agencies also prohibit portable hard drives (41%), PDAs (41%), mobile phones/MP3s/iPods (38%) and USB/portable flash memory (38%).
- ◆ Two-fifths (40%) of agencies do not prohibit any private PSDs in the workplace.
 - Smaller agencies were the most likely to not prohibit any private PSDs – 60% of very small agencies, 43% of small agencies, 38% of medium agencies and 25% of large agencies.

3.3.2. Controls on the use of private PSDs

Figure 10 shows that agencies were more likely to use software controls¹⁵ than hardware controls¹⁶ to restrict or control the use of private PSDs in the workplace.

- ◆ Just over half of agencies indicated that they use software controls (54%) to restrict or control the use of private PSDs, with the most common method being operating system controls (69%).
 - 48% of agencies that did not currently have software controls in place intended to introduce them in the next 12 months.
 - 57% of agencies that did not have software controls in place nor intended to introduce them in the next 12 months indicated that this was because the lack of such controls was low risk for their agency, while 13% said it was cost prohibitive.
- ◆ Only 16%¹⁷ of agencies indicated that they use hardware controls to restrict or control the use of private PSDs, with the most common method being the physical disabling of USB ports (38% of agencies with hardware controls).

¹⁵ See glossary in Appendix A for a definition of software controls.

¹⁶ See glossary in Appendix A for a definition of hardware controls.

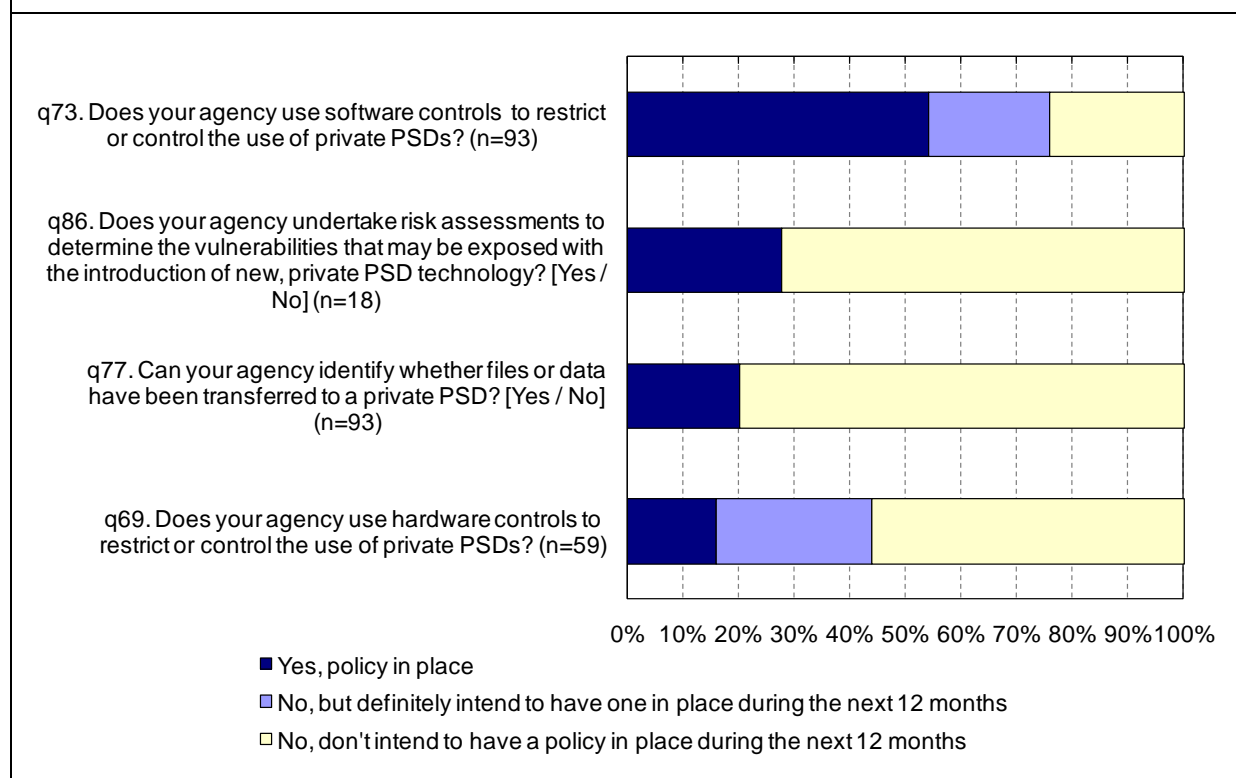
¹⁷ Agencies that did not answer this question but that indicated that they allow PSDs to be used in the workplace were interpreted as having no hardware controls.

- 33% of agencies that did not currently have hardware controls in place intended to introduce them in the next 12 months.
 - 45% of agencies that did not have hardware controls in place nor intended to introduce them in the next 12 months indicated that this was because the lack of such controls was low risk for their agency, while 22% said it was cost prohibitive.

Figure 10 also shows that well under half of agencies indicated that they can identify when data is transferred to a private PSD, or conduct risk assessments about new private PSD technologies.

- ◆ 28% of agencies that did not have a private PSD usage policy, nor intended to develop one in the next 12 months (five agencies or 5% of all agencies) indicated that they conduct risk assessments to determine vulnerabilities that may be exposed with the introduction of new, private PSD technology.
- ◆ 20% of agencies indicated that they could identify whether files or data have been transferred to a private PSD.

Figure 10: Extent to which agencies have controls on the use of private PSDs
(% of agencies)



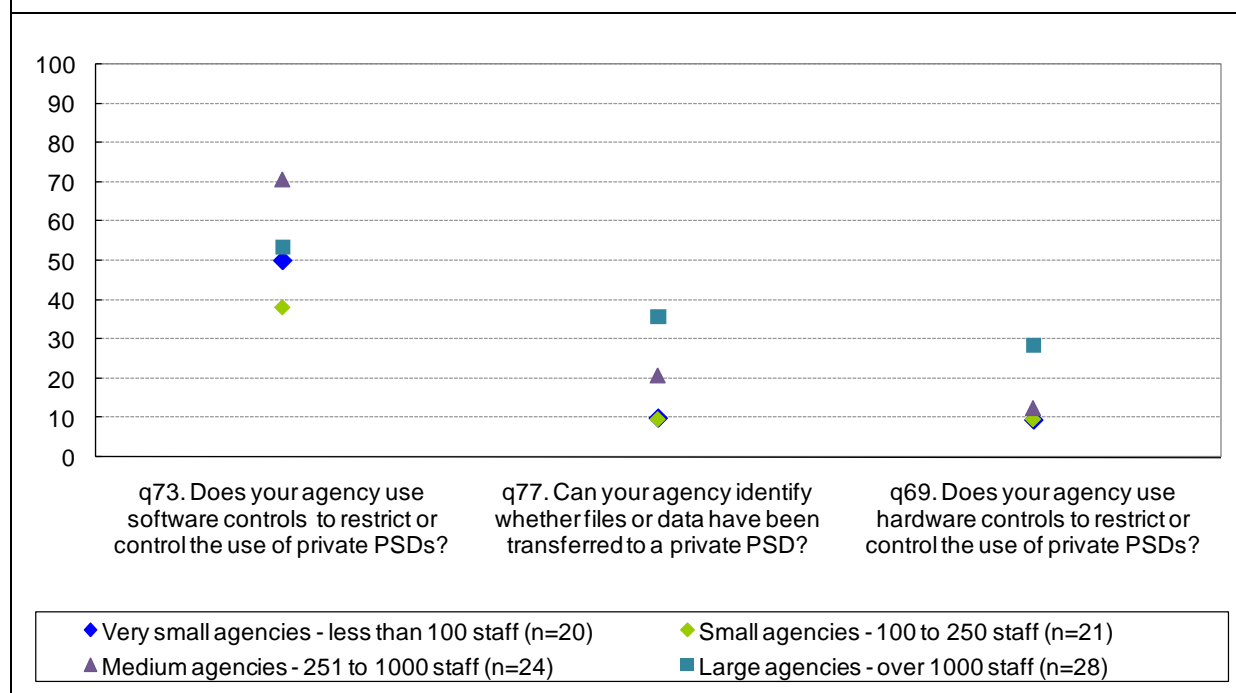
Controls on the use of private PSDs by agency size

Controls on the use of private PSDs tended to be greater for larger agencies in most cases. Figure 11 shows that:

- ◆ 71% of medium agencies used software controls on private PSDs, compared with around half of large (54%) and very small (50%) agencies and well under half (38%) of small agencies;
- ◆ the capability to identify whether files or data have been transferred to a private PSD was greater amongst large agencies (36%), than medium (21%), small or very small agencies (both 10%); and
- ◆ 29% of large agencies used hardware controls on private PSDs, compared with 13% of medium agencies and 10% of small and very small agencies.

Figure 11: Extent to which agencies have controls¹⁸ on the use of private PSDs by agency size

(% of agencies that answered 'yes' by agency size)



¹⁸ The comparison of risk assessments of new private PSD technologies by agency size is not shown on this chart due to the very small number of agencies that answered this question in each size category (between 3 and 7).

3.3.3. Training provided to staff on private PSD usage

Around one quarter of agencies that allow private PSD usage indicated that they provide staff with training on the use of private PSDs in the workplace and relevant security requirement (24%), with the most common delivery methods being specific formal training (47%) and on-the-job training (47%).

- ◆ 44% of agencies with at least one office outside Australia indicated that they provided staff with training, compared with 20% of agencies with no offices outside Australia.

3.3.4. Loss or theft of private PSDs

Less than one-fifth of agencies (18%) indicated that they had experienced the loss or theft of privately owned PSDs that had been used to store personal information held by the agency in the previous 12 months.

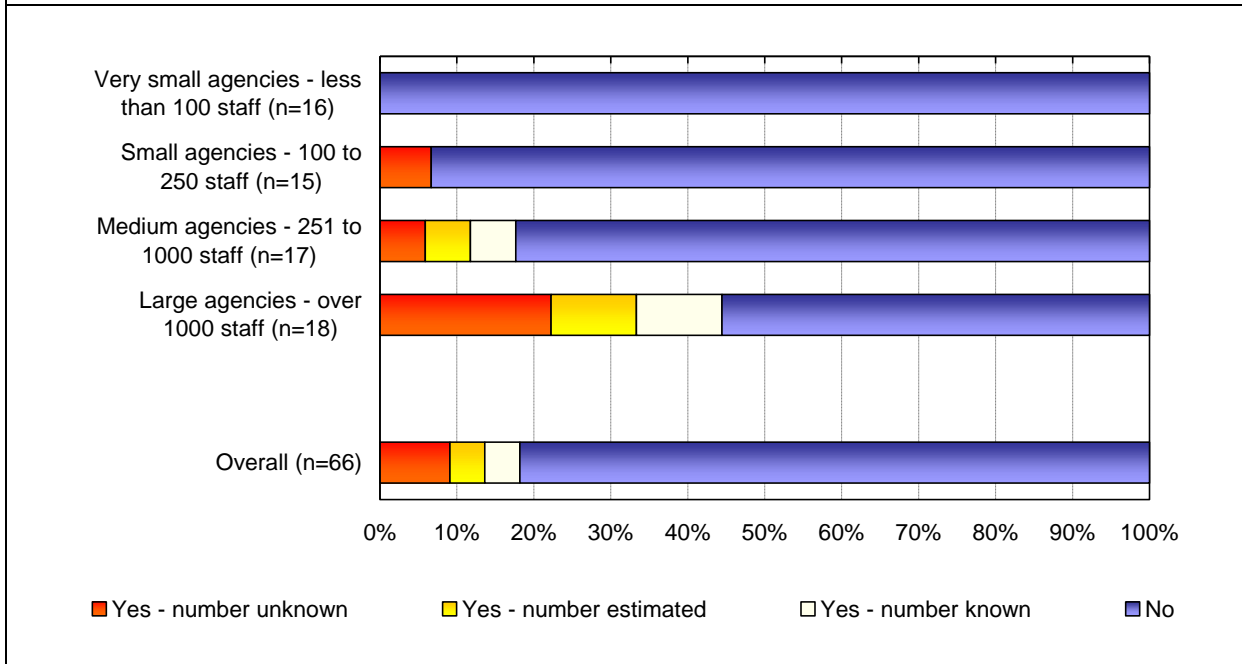
- ◆ Six of these agencies (50%) were able to estimate the number of private PSDs lost or stolen over this period. Five of these agencies indicated that between 1 and 3 private PSDs had been lost or stolen from their agency over this period, while the other agency¹⁹ estimated that 32 private PSDs has been lost or stolen in their agency.
- ◆ 80% of agencies that had a private PSD lost or stolen over this period found out about this by being notified by staff.
 - As indicated in Section 3.1 on page 19, several agencies with no policies in place on the loss or theft of private PSDs indicated that they had no way of knowing if private PSDs had been lost or stolen in their agency. The above results on the extent of loss or theft of private PSDs may therefore understate the true extent of this issue, due to potential under-reporting in these agencies.

Large agencies and agencies engaging more than 50 CSP staff experienced the highest incidence of loss or theft of private PSDs.

- ◆ Figure 12 shows that 44% of large agencies experienced the loss or theft of private PSDs, compared with 18% of medium agencies, 7% of small agencies and no very small agencies.
- ◆ 55% of agencies that engaged more than 50 CSP staff experienced the loss or theft of a private PSD.

¹⁹ This was a large agency that had a documented policy in place for reporting the loss or theft of private PSDs that may have been used to store personal information belonging to the agency. This agency prohibited the use of the all types of private PSDs in the workplace except PDAs and CDs / DVDs.

Figure 12: Loss or theft of private PSDs
(% of agencies)





Appendix A: Glossary



Glossary

Portable Storage Device ('PSD')	Also known as a 'removable storage device'. A small, lightweight, portable, easy to use device, capable of storing and transferring large volumes of data. This device is either exclusively used for data storage (e.g. Portable external hard drives, CDs/DVDs, USBs) or is capable of multiple other functions (e.g. Laptops/ notebooks, Personal Digital Assistants (PDAs - such as Pocket PC, Palm, BlackBerry) and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones).
Contracted Service Providers ('CSP')	As outlined in Section 6 of the Privacy Act 1988 a contracted service provider, for a government contract, means: (a) an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or (b) a subcontractor for the government contract.
'Wireless' interface	Wireless communication describes telecommunications in which electromagnetic waves (rather than wire) carry the signal over part of, or over the entire communication path. Personal computers are increasingly connecting through wireless means, as opposed to the traditional 'wired' means.
USB interface	Universal Serial Bus ('USB') is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports which enable many devices to be connected using a single standardised interface socket. Devices can be connected and disconnected without rebooting the computer or turning off the device.
FireWire	FireWire (IEEE 1394 standard) is an interface for high-speed communications and data transfer. It is the preferred transfer mechanism for almost all high end professional audio and video equipment, and many personal computers intended for home or professional audio/video use have built-in FireWire port/s.
USB key	Also known as "flash drive", "USB stick", "memory key". A device that plugs into the computer's USB port. Small enough to hook onto a key-ring, it allows data to be easily downloaded.
Personal Digital Assistant ('PDA')	A small, mobile, hand-held device such as Pocket PC, Palm and BlackBerry, which provides computing and data storage/retrieval capabilities for personal and business use.
Hardware controls	Hardware controls may include physically disconnecting, removing or sealing off ports, using non-standard locking ports, or other measures.
Software controls	Software controls may include installing specific control software, firewalls, system policies, or operating system controls.



'Native' encryption	Encryption is the process of systemically encoding data before transmission and during storage, so that an unauthorised party cannot decipher it. 'Native' encryption software comes included on the PSD as purchased. Many brands of USB key now come with native encryption.
Operating system controls	Built-in controls found in an operating system (e.g. Windows) that allows administrators to manage access and security of software or devices attached to a personal computer.
Endpoint security	Security software that is distributed to end-user devices (e.g. PCs, laptops) but centrally managed. Endpoint security software provides services such as anti-virus and controlling access to attached devices (e.g. PSDs).
Netbook	A light-weight, low-cost, very portable laptop aimed at web browsing, email and general purpose web-based applications.
Privacy Enhancing Technology (PET)	PET is a system of technology measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data.





Appendix B: Survey Questionnaire





Australian Government
Office of the Privacy Commissioner



Office of the Privacy Commissioner

PSD Survey

2009



Australian Government
Office of the Privacy Commissioner



Introduction

What is the purpose of this survey?

The survey aims to identify the privacy controls that govern how personal information is transferred both within and between Australian public sector agencies, and external organisations.

The survey also aims to identify the current privacy controls that Australian public sector agencies have in place around the use of Portable Storage Devices (PSDs), both those issued by an agency to staff and those privately owned by staff.

Why does the Office of the Privacy Commissioner (OPC) need this information?

The widespread availability and access to PSDs raise a number of privacy and security challenges for Australian public sector agencies, especially around the storage and security of personal information under Information Privacy Principle 4. These challenges arise both from the technical capacities of PSDs (i.e. high storage, fast speed of transfer, 'plug and play' functionality) as well as the physical characteristics of many devices (i.e. small size, light weight, low cost, high portability).

The information will be used by the OPC to identify good privacy practices and policies, as well as identify any areas of concern that may need to be addressed across Australian public sector agencies. The information gathered will also inform the development of future guidance material by the OPC to assist Australian public sector agencies to maintain appropriate policies and procedures to minimise the risks presented by the use of PSDs

Who is conducting the survey?

ORIMA Research Pty Ltd has been engaged by the Australian Privacy Commissioner to conduct an online (electronic) survey of Australian public sector agencies.

Which agencies should respond to this survey?

All Australian Government agencies subject to the Public Service Act 1999 should respond to this survey. All bodies subject to the Commonwealth Authorities and Companies Act 1997 (CAC Act) that have been directed by the relevant Minister to comply with Australian Government privacy policies should also respond to this survey; other CAC Act bodies are encouraged to do so.

Who in my agency should complete the survey?

The majority of the survey relates to the information and privacy policies, procedures and controls that your agency has in place in relation to the handling of records containing personal information. As such, in the first instance a link to the survey will be sent to your agency's Privacy Contact Officer (PCO). If your agency does not have a PCO, your agency will nominate an appropriate individual to respond.

I am the nominated Officer – what do I have to do?

You will need to:

- Act as the primary point of contact for your agency on all issues relating to the survey
- Complete the relevant sections of the questionnaire on behalf of your agency
- Liaise with relevant areas of your agency (e.g. Personnel, Information Technology areas)
- Coordinate the response to the survey across your agency
- Ensure your agency's survey response is completed/ submitted online by 20 March 2009.

How is the information used?

The information will be used by the OPC to compile a public sector-wide level report on the current use of Personal Storage Devices (PSDs) across Australian Government agencies. No individual agencies will be identifiable in the consolidated report. Individual agency-level feedback may also be provided to participating agencies by the OPC.

When is the survey due?

A completed survey response for each agency is required by **20 March 2009**.

Instructions

How should the survey be completed?

1. Read each question carefully.
2. Where options have been provided, select the response that represents the answer you want to give. For example, if your agency provides access to or issues PSDs to agency staff only, mark option 1 as shown below:

Does your agency provide access to / issue any of your staff with PSDs?

- 1 Yes – agency staff only
- 2 Yes – both agency and CSP staff
- 3 No [\[go to question 27\]](#)

3. Where multiple answers apply, select each applicable answer.

Further Information

All queries regarding completing the survey should be directed to the Andrew Lenihan of ORIMA Research.

telephone: (02) 6175 1000

email: andrew.lenihan@orima.com

Glossary

Portable Storage Device ('PSD')	Also known as a 'removable storage device'. A small, lightweight, portable, easy to use device, capable of storing and transferring large volumes of data. This device is either exclusively used for data storage (e.g. Portable external hard drives, CDs/DVDs, USBs) or is capable of multiple other functions (e.g. Laptops/ notebooks, Personal Digital Assistants (PDAs - such as Pocket PC, Palm, BlackBerry) and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones).
'Wireless' interface	Wireless communication describes telecommunications in which electromagnetic waves (rather than wire) carry the signal over part of, or over the entire communication path. Personal computers are increasingly connecting through wireless means, as opposed to the traditional 'wired' means.
USB interface	Universal Serial Bus ('USB') is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports which enable many devices to be connected using a single standardised interface socket. Devices can be connected and disconnected without rebooting the computer or turning off the device.
FireWire	FireWire (IEEE 1394 standard) is an interface for high-speed communications and data transfer. It is the preferred transfer mechanism for almost all high end professional audio and video equipment, and many personal computers intended for home or professional audio/video use have built-in FireWire port/s.
USB key	Also known as "flash drive", "USB stick", "memory key". A device that plugs into the computer's USB port. Small enough to hook onto a key-ring, it allows data to be easily downloaded.
Personal Digital Assistant ('PDA')	A small, mobile, hand-held device such as Pocket PC, Palm and BlackBerry, which provides computing and data storage/retrieval capabilities for personal and business use.
Hardware controls	Hardware controls may include physically disconnecting, removing or sealing off ports, using non-standard locking ports, or other measures.
Software controls	Software controls may include installing specific control software, firewalls, system policies, or operating system controls.
'Native' encryption	Encryption is the process of systemically encoding data before transmission and during storage, so that an unauthorised party cannot decipher it. 'Native' encryption software comes included on the PSD as purchased. Many brands of USB key now come with native encryption.
Operating system controls	Built-in controls found in an operating system (e.g. Windows) that allows administrators to manage access and security of software or devices attached to a personal computer.



Endpoint security	Security software that is distributed to end-user devices (e.g. PCs, laptops) but centrally managed. Endpoint security software provides services such as anti-virus and controlling access to attached devices (e.g. PSDs).
Netbook	A light-weight, low-cost, very portable laptop aimed at web browsing, email and general purpose web-based applications.
Privacy Enhancing Technology (PET)	PET is a system of technology measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data.



A. Preliminary – Demographic Details

1. Agency Name:

.....

- | | Australia only | Australia and overseas |
|---|----------------|------------------------|
| 2. Where is your agency primarily located? | 1 | 2 |
| 3. Please indicate the total number of agency office locations... | | |
| a. ...within Australia | n= _____ | |
| b. ...outside of Australia | n= _____ | |

The next question relates to the number of staff employed by your agency. This includes both on-going and non-ongoing (i.e. temporary contract) staff.

4. What was the total number of staff (head count of both on-going and non-ongoing) employed by your agency as at 31 December 2008? n= _____
- Note: An Approximate number is sufficient.

The next questions relate to staff from Contracted Service Providers (CSPs), who may have access to your agency's information resources, including personal information.

5. If known, please indicate:
- a. The total number of CSP staff (head count) engaged by your agency as at 31 December 2008? 1. (n= _____) 2. Don't know
- Note: An Approximate number is sufficient.
- [Go to q6]
- b. The total number of CSP organisations engaged by your agency as at 31 December 2008? 1. (n= _____) 2. Don't know
6. Please provide the following information:
Note: This will only be used if we need to contact you to clarify any of your survey responses.

a. Contact officer's name	
b. Contact phone number	
c. Contact email address	

B. General Transfers of Personal Information

Transfers of personal information within your agency

	Yes	No
7. Does your agency have a policy* in place to address the secure transfer of <i>records containing personal information</i> within your agency? (e.g. between different business areas, or different office locations within your agency)	1	2 [Go to q11]

* Throughout this questionnaire the term 'policy' refers to any policies, guidelines or written procedures developed by your agency to guide staff.

8. Does this policy cover: **[Select all that apply]**

- 1 Physical (i.e. hard-copy) records
- 2 Electronic records
- 3 Other **[Please specify]**

9. Please provide the title/name of this Policy:

Please provide the names of up to five relevant policies if your agency has more than one.

- 1
- 2
- 3
- 4
- 5

10. If required, would you be able to provide a copy of this policy / these policies to the OPC?

Yes	No
1	2
Go to question 13	

11. Does your agency intend to develop a policy around the transfer of records containing personal information within your agency **during the next 12 months?**

Yes – definitely	Yes – probably	No
1	2	3
Go to question 13		

12. What is the **main** reason your agency does not intend to develop such a policy? **[Please select one only]**

- 1 Cost prohibitive
- 2 Low risk
- 3 Other **[Please specify]**



Transfers of personal information outside your agency

- | | Yes | No | | | | | | | | | |
|--|---|------------------|----------------|----|---|--------------------------|---|--------------------------|--|--|--|
| 13. Does your agency have a policy in place to address the secure transfer of <i>records containing personal information</i> outside your agency? (e.g. to other Commonwealth or State Government agencies, private sector organisations (including CSPs and staff) or individuals.) | 1 | 2
[Go to q17] | | | | | | | | | |
| 14. Does this policy cover: [Select all that apply] | | | | | | | | | | | |
| 1 Physical (i.e. hard-copy) records | | | | | | | | | | | |
| 2 Electronic records | | | | | | | | | | | |
| 3 Other [Please specify] | | | | | | | | | | | |
| 15. Please provide the title/name of this Policy:
Please provide the names of up to five relevant policies if your agency has more than one. | | | | | | | | | | | |
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 5 | | | | | | | | | | | |
| 16. If required, would you be able to provide a copy of this policy / these policies to the OPC? | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; text-align: center;">Yes</th> <th style="width: 50%; text-align: center;">No</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">2</td> </tr> <tr> <td colspan="2" style="text-align: center;">Go to question 19</td> </tr> </tbody> </table> | Yes | No | 1 | 2 | Go to question 19 | | | | | |
| Yes | No | | | | | | | | | | |
| 1 | 2 | | | | | | | | | | |
| Go to question 19 | | | | | | | | | | | |
| 17. Does your agency intend to develop a policy around the transfer of records containing personal information between your agency and external parties during the next 12 months? | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%; text-align: center;">Yes – definitely</th> <th style="width: 33%; text-align: center;">Yes – probably</th> <th style="width: 34%; text-align: center;">No</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">2</td> <td style="text-align: center;">3</td> </tr> <tr> <td colspan="3" style="text-align: center;">Go to question 19</td> </tr> </tbody> </table> | Yes – definitely | Yes – probably | No | 1 | 2 | 3 | Go to question 19 | | | |
| Yes – definitely | Yes – probably | No | | | | | | | | | |
| 1 | 2 | 3 | | | | | | | | | |
| Go to question 19 | | | | | | | | | | | |
| 18. What is the main reason your agency does not intend to develop such a policy? [Please select one only] | | | | | | | | | | | |
| 1 Cost prohibitive | | | | | | | | | | | |
| 2 Low risk | | | | | | | | | | | |
| 3 Other [Please specify] | | | | | | | | | | | |

Transfers of personal information involving staff working from home

- | | Yes | No | | |
|--|------------------------|------------------|--|----|
| 19. Does your agency have a policy in place to address the secure transfer of <i>records containing personal information</i> for staff temporarily working away from the office (e.g. working from home, at airports or hotels)? | 1 | 2
[Go to q23] | | |
| 20. Does this policy cover: [Select all that apply] | | | | |
| 1 Physical (i.e. hard-copy) records | | | | |
| 2 Electronic records | | | | |
| 3 Other [Please specify] | | | | |
| 21. Please provide the title/name of this Policy:
Please provide the names of up to five relevant policies if your agency has more than one. | | | | |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 22. If required, would you be able to provide a copy of this policy / these policies to the OPC? | | | | |
| | 1 | 2 | | |
| | Go to Section C | | | |
| 23. Does your agency intend to develop a policy around the transfer of records containing personal information for your staff working from home during the next 12 months? | | | | |
| | Yes – definitely | Yes – probably | No – covered by a more general guideline | No |
| | 1 | 2 | 3 | 4 |
| | Go to Section C | | | |
| 24. What is the main reason your agency does not intend to develop such a policy? [Please select one only] | | | | |
| 1 Cost prohibitive | | | | |
| 2 Low risk | | | | |
| 3 Other [Please specify] | | | | |

C. Use of Agency-Issued PSDs

This section covers both staff directly employed by your agency (i.e. on-going and non-going), as well as staff from CSPs who may have access to your agency's information resources, including personal information.

For the purposes of the survey, Portable Storage Devices (PSDs) are defined to include:

- ◆ Laptop/ notebook computers;
- ◆ Portable external hard drives;
- ◆ Personal Digital Assistants (PDAs), such as Pocket PC, Palm, BlackBerry;
- ◆ CDs/ DVDs;
- ◆ Portable flash memory (often referred to as USB keys, USB sticks, or memory sticks); and
- ◆ Devices with in-built accessible storage, including MP3 players, iPods, and mobile phones.

25. Does your agency provide access to / issue any of your staff with PSDs?

- 1 Yes – agency staff only
- 2 Yes – both agency and CSP staff
- 3 No [\[go to Section D\]](#)

26. What type of PSDs are provided? [\[Select all that apply\]](#)

- 1 Laptops / notebooks
- 2 Portable hard drives
- 3 CDs / DVDs
- 4 PDAs
- 5 Mobile phone / MP3 / iPod
- 6 USB/ Portable flash memory
- 7 Other [\[Please specify\]](#)

	Yes	No
27. Does your agency have specific policies in place to govern the use of agency-issued PSDs by your staff?	1	2 [Go to q33]

28. If so, does the policy cover:

- 1 All PSDs
- or Specific PSDs only: [\[Select all that apply\]](#)
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other [\[Please specify\]](#)



29. Please provide the title/name of this Policy:
Please provide the names of up to five relevant policies if your agency has more than one.

1

2

3

4

5

- | | Yes | No |
|--|-----|----|
| 30. If required, would you be able to provide a copy of this policy / these policies to the OPC? | 1 | 2 |

- | | Yes | No |
|---|-----|----|
| 31. Does the policy prescribe how agency data containing personal information is to be deleted from PSDs? | 1 | 2 |

32. How do you ensure your staff are made aware of this policy? **[Select all that apply]**

- 1 All staff provided with a copy
- 2 Manager's responsibility
- 3 Staff responsibility (e.g. sign Acceptable Use agreement)
- 4 Induction training
- 5 Group email
- 6 Policy on intranet site
- 7 Other **[Please specify]**


Please go to
question 35

- | | Yes | No |
|---|-------------------------|----|
| 33. Does your agency intend to develop a policy around the use or control of agency-issued PSDs during the next 12 months? | 1
[Go to q35] | 2 |

34. What is the **main** reason your agency does not intend to develop such a policy? **[Please select one only]**

- 1 No agency-issued PSDs
- 2 Cost prohibitive
- 3 Low risk
- 4 Other **[Please specify]**

	Yes	No
35. Does your agency provide staff with training on the use of agency-issued PSDs and relevant security requirements?	1	2 [Go to q37]
36. What sort of training do you provide: [Select all that apply]		
1	Specific formal training	
2	Self-paced online training	
3	On the job training	
4	Other [Please specify]	
	Yes	No
37. Does your agency keep a register ¹ of agency-issued PSDs?	1	2 [Go to q42]
38. If so, does the register cover:		
1	All PSDs	
	or Specific PSDs only: [Select all that apply]	
2	Laptops/notebooks	
3	Portable hard drives	
4	CDs / DVDs	
5	PDAs	
6	Mobile phone / MP3 / iPod	
7	USB/ Portable flash memory	
8	Other [Please specify]	
	Yes	No
39. Does your agency undertake an annual stocktake of the register of agency-issued PSDs?	1	2 [Go to q41]
40. If so, does the stocktake cover:		
1	All PSDs	
	or Specific PSDs only: [Select all that apply]	
2	Laptops/notebooks	
3	Portable hard drives	
4	CDs / DVDs	
5	PDAs	
6	Mobile phone / MP3 / iPod	
7	USB/ Portable flash memory	
8	Other [Please specify]	



Please go to question 42

¹ A register refers to any list (including but not limited to an asset register) that may be made when agency-issued PSDs are purchased, issued or returned by staff.

41. Why does your agency not undertake such an annual stocktake? **[Select all that apply]**

- 1 Low cost item²
- 2 Cost prohibitive
- 3 Low risk
- 4 Other **[Please specify]**

	Yes	No
42. Are staff who are issued with agency PSDs required to sign an agreement with the agency around their acceptance of the terms and conditions of use of the PSD (i.e. an Acceptable Use agreement)?	1	2 [Go to q45]

43. What types of PSDs require a signed agreement?

- 1 All PSDs
or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

	Yes	No
44. Does this agreement/do <u>all</u> these agreements specify the staff member agrees to adhere to relevant Agency and Australian Government policies and procedures (e.g. Protective Security Manual, Chief Executive Guidance, <i>Australian Government ICT Security Manual</i> (ACSI 33))?	1	2

	Yes	No
45. Are agency-issued PSDs required to have a minimum standard of encryption?	1	2 [Go to q49]

² Asset registers may use a threshold that precludes PSDs from being considered (due to the relatively low cost of some PSDs). Asset register methodology may still be relevant if the PSD is defined as an 'attractive item'.

46. Please nominate which devices are required to be encrypted:

- 1 All PSDs
- or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

	Supplied with the device (i.e. native encryption)	Provided by your agency	Both
47. Is this PSD encryption:	1	2	3

	Yes	No	Don't know
48. Does this PSD encryption allow for the storage of non-encrypted data?	1	2	3

49. Products that control the way PSDs are used may include the ability to track data transfers to a device. Operating system controls and audit logs may also provide information on when files or data are transferred to a PSD.

Can your agency identify whether files or data have been transferred to an agency-issued PSD?

- 1 Yes – from all PSDs
- 2 Yes – from some PSDs, please specify which ones:

- 3 No

50. The Protective Security manual (PSM) requires that, if information is security classified, then any media or device storing that information must be classified to at least the same level.

	Yes – as per the PSM	No
Are agency-issued PSDs classified in line with your agency's Information Classification Scheme (e.g. the PSM)?	1	2

	Yes	No
51. Are agency-issued PSDs labelled clearly with a warning against unauthorised use?	1	2 [Go to q53]



52. Please nominate which devices are labelled with a warning against unauthorised use:

- 1 All PSDs
- or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

	Yes	No
53. Are agency-issued PSDs clearly labelled, asking the finders of a lost PSD to hand the equipment in to any Australian Police station or, if overseas, an Australian Embassy, Consulate or High Commission?	1	2 [Go to q55]

54. Please nominate which devices are labelled in this way:

- 1 All PSDs
- or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

	Yes	No
55. Does your agency have a documented policy for reporting the loss or theft of an agency-issued PSD?	1	2 [Go to q60]

56. Is this policy: **[Select one only]**

- 1 Part of a general loss/ incident reporting policy **[Go to q58]**
- 2 A specific PSD loss/ incident policy

57. What types of PSD does this policy cover?

- 1 All PSDs
- or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

58. Please provide the title/name of this Policy:

Please provide the names of up to five relevant policies if your agency has more than one.

- 1
- 2
- 3
- 4
- 5

59. If required, would you be able to provide a copy of this policy / these policies to the OPC?

Yes	No
1	2
Go to question 61	

60. How does your agency identify when an agency-issued PSD has been lost or stolen?

.....

.....

.....

.....

61. In the past 12 months, has your agency experienced any losses or thefts of agency-issued PSDs?

- 1 Yes – number **known** as: _____
- 2 Yes – number **estimated** as: _____
- 3 Yes – number unknown
- 4 No **[Go to question 63]**

62. How did your agency first become aware of the loss or theft of agency-issued PSDs that had been used to store personal information held by the Agency? **[Select all that apply]**

- 1 Staff notified agency
- 2 Public notified agency
- 3 Media notified agency
- 4 Server/ Firewall detection
- 5 Agency intrusion/ prevention systems
- 6 Other **[Please specify]**

63. Does your agency have a documented policy which covers the disposal of agency-issued PSDs that are obsolete or no longer required?

Yes

No

1

2

**[Go to
Section D]**

64. Is this policy: **[Select one only]**

- 1 Part of a general disposal policy **[Go to Section D]**
- 2 A specific PSD disposal policy

65. What types of PSD does this policy cover?

- 1 All PSDs
- or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
 - 3 Portable hard drives
 - 4 CDs / DVDs
 - 5 PDAs
 - 6 Mobile phone / MP3 / iPod
 - 7 USB/ Portable flash memory
 - 8 Other **[Please specify]**



D. Use of Private PSDs

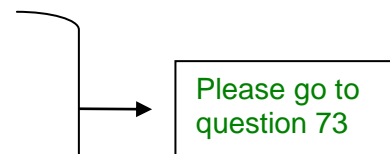
This section covers the use of private PSDs within the agency workplace. Private PSDs are not provided or issued by an agency to staff – they are usually owned/ used by an individual staff member. Staff who own or use a private PSD in the workplace may be able to access data and information (including personal information) held in an agency's IT system in some circumstances.

	Yes – all private PSDs prohibited	Yes – some private PSDs prohibited	No – no private PSDs prohibited
66. Does your agency prohibit the use of any type of private PSD in the workplace?	1 [Go to q69]	2	3 [Go to q68]
67. What types of PSDs are prohibited ? [Select all that apply]			
1 Laptops/notebooks			
2 Portable hard drives			
3 CDs / DVDs			
4 PDAs			
5 Mobile phone / MP3 / iPod			
6 USB/ Portable flash memory			
7 Other [Please specify]			
68. Are there any restrictions placed on private PSDs before they are allowed to be used? [Select all that apply]			
1 Yes – require manager agreement			
2 Yes – sign acceptable use policy			
3 Yes – add to register			
4 Other [Please specify]			
5 No			
69. Does your agency use hardware controls ³ to restrict or control the use of private PSDs?	Yes 1		No 2 [Go to q71]

³ Hardware controls may include physically disconnecting, removing or sealing off ports, using non-standard locking ports or other measures.

70. Is this done by: **[Select all that apply]**

- 1 Physically disabling USB ports
- 2 Removing ports
- 3 Sealing ports
- 4 Using non-standard locking ports
- 5 Other **[Please specify]**



71. Does your agency intend to *implement* hardware controls for private PSDs during the next 12 months?

Yes	No
1 [Go to q73]	2

72. What is the **main** reason your agency does not intend to implement such controls? **[Please select one only]**

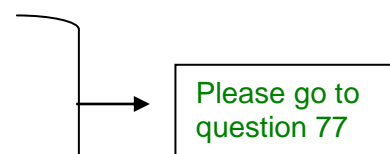
- 1 Cost prohibitive
- 2 Low risk
- 3 Other **[Please specify]**

73. Does your agency use software controls⁴ to restrict or control the use of private PSDs?

Yes	No
1	2 [Go to q75]

74. Is this done by: **[Select all that apply]**

- 1 Installing specific control software
- 2 Firewalls
- 3 Operating system controls
- 4 Other **[Please specify]**



75. Does your agency intend to *implement* software controls for private PSDs during the next 12 months?

Yes	No
1 [Go to q77]	2

76. What is the **main** reason your agency does not intend to implement such controls? **[Please select one only]**

- 1 Cost prohibitive
- 2 Low risk
- 3 Other **[Please specify]**

⁴ Software controls may include installing specific control software, firewalls or operating system controls (such as locking down the environment to prevent users installing driver software).

77. Products that control the way PSDs are used may include the ability to track data transfers to a device. Operating system controls and audit logs may also provide information on when files or data are transferred to a PSD.

	Yes	No
Can your agency identify whether files or data have been transferred to a private PSD?	1	2

	Yes	No
78. Does your agency have specific policies in place to govern the use of private PSDs by your staff?	1	2 [Go to q84]

79. Does this policy cover:
- 1 All PSDs
 - or Specific PSDs only: **[Select all that apply]**
 - 2 Laptops/notebooks
 - 3 Portable hard drives
 - 4 CDs / DVDs
 - 5 PDAs
 - 6 Mobile phone / MP3 / iPod
 - 7 USB/ Portable flash memory
 - 8 Other **[Please specify]**

80. Please provide the title/name of this Policy:
Please provide the names of up to five relevant policies if your agency has more than one.

- 1
- 2
- 3
- 4
- 5

	Yes	No
81. If required, would you be able to provide a copy of this policy / these policies to the OPC?	1	2

82. How do you ensure your staff are made aware of this policy? **[Select all that apply]**

- 1 All staff provided with a copy
- 2 Manager's responsibility
- 3 Staff responsibility (e.g. sign Acceptable Use agreement)
- 4 Induction training
- 5 Group email
- 6 Policy on intranet site
- 7 Other **[Please specify]**

83. Does the policy prescribe how agency data containing personal information stored on a private PSD is to be deleted?

Yes	No	Not applicable
1	2	3
Go to instruction before question 88		

84. Does your agency intend to develop a policy around use of private PSDs by your staff **during the next 12 months?**

Yes	No
1	2
[Go to instruction before q88]	

85. What is the **main** reason your agency does not intend to develop such a policy? **[Please select one only]**

- 1 Private PSDs prohibited
- 2 Cost prohibitive
- 3 Low risk
- 4 Other **[Please specify]**

86. Does your agency undertake risk assessments to determine the vulnerabilities that may be exposed with the introduction of new, private PSD technology?

Yes	No
1	2
[Go to instruction before q88]	

87. Please nominate which new technology devices are risk assessed:

- 1 All PSDs
or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives
- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

If your agency prohibits the use of **all** types of private PSDs (you answered option 1 in question 66), please go to question 96.

	Yes	No	Not applicable
88. Does your agency provide staff with training on the use of private PSDs in the workplace and relevant security requirements?	1	2	3
		Go to question 90	

89. What sort of training do you provide: **[Select all that apply]**

- 1 Specific formal training
- 2 Self-paced online training
- 3 On the job training
- 4 Other **[Please specify]**

	Yes	No	Not applicable
90. Does your agency have a documented policy for reporting the loss or theft of a private PSD that may have been used to store personal information belonging to the Agency?	1	2 [Go to question 95]	3 [Go to question 96]

91. Is this policy: **[Select one only]**

- 1 Part of a general loss/ incident reporting policy
- 2 A specific PSD loss/ incident policy

92. What types of PSD does this policy cover?

- 1 All PSDs
or Specific PSDs only: **[Select all that apply]**
- 2 Laptops/notebooks
- 3 Portable hard drives



- 4 CDs / DVDs
- 5 PDAs
- 6 Mobile phone / MP3 / iPod
- 7 USB/ Portable flash memory
- 8 Other **[Please specify]**

93. Please provide the title/name of this Policy:
 Please provide the names of up to five relevant policies if your agency has more than one.

- 1
- 2
- 3
- 4
- 5

94. If required, would you be able to provide a copy of this policy / these policies to the OPC?

Yes	No
1	2
Go to question 96	

95. How does your agency identify when a private PSD (that may have been used to store personal information belonging to the Agency) has been lost or stolen?

-
-
-
-

96. In the past 12 months, has your agency experienced any losses or thefts of privately owned PSDs that have been used to store personal information held by the Agency?

- 1 Yes – number **known** as: _____
- 2 Yes – number **estimated** as: _____
- 3 Yes – number unknown
- 4 No
- 5 Not applicable

Go to Section E

97. How did your agency first become aware of the loss or theft of privately owned PSDs that had been used to store personal information held by the Agency? **[Select all that apply]**

- 1 Staff notified agency
- 2 Public notified agency
- 3 Media notified agency
- 4 Server/ Firewall detection
- 5 Agency intrusion/ prevention systems
- 6 Other **[Please specify]**

E. General

98. If you have comments on any part of this survey or wish to provide extra information, please do so here.

If your comments relate to specific questions, the relevant question numbers should be indicated.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

99. **Thank you for completing this survey.** To assist with future surveys, please estimate the time taken for your agency to complete this survey. Include the time spent by staff in reading the instructions, working on the questions and obtaining the required information.

1 _____ hours _____ minutes



Appendix C: List of Agencies that Completed the Survey



List of Agencies that Completed the Survey

Aboriginal Hostels Limited
Airservices Australia
Attorney General's Department
AUSTRAC
Austrade
Australian Agency for International Development
Australian Broadcasting Corporation
Australian Bureau of Statistics
Australian Business Arts Foundation
Australian Centre for International Agricultural Research
Australian Communications and Media Authority
Australian Competition and Consumer Commission
Australian Customs Service
Australian Electoral Commission
Australian Fair Pay Commission Secretariat
Australian Film, Television and Radio School
Australian Fisheries Management Authority
Australian Hearing
Australian Human Rights Commission
Australian Industrial Registry
Australian Institute of Aboriginal and Torres Strait Islander Studies
Australian Institute of Family Studies
Australian Law Reform Commission
Australian National Audit Office
Australian National Maritime Museum
Australian Pesticides and Veterinary Medicines Authority
Australian Postal Corporation
Australian Prudential Regulation Authority
Australian Public Service Commission
Australian Research Council
Australian Securities and Investments Commission
Australian Sports Anti-Doping Authority
Australian Taxation Office
Bureau of Meteorology
Centrelink
Civil Aviation Safety Authority
Comcare
Commonwealth Grants Commission
Commonwealth Scientific and Industrial Research Organisation
Commonwealth Superannuation Administration
CrimTrac
CRS Australia
Department of Agriculture, Fisheries and Forestry



Department of Broadband, Communications and the Digital Economy
Department of Climate Change
Department of Defence
Department of Education, Employment and Workplace Relations
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Finance and Deregulation
Department of Foreign Affairs and Trade
Department of Human Services
Department of Infrastructure, Transport, Regional Development and Local Government
Department of Innovation, Industry, Science and Research
Department of Resources, Energy and Tourism
Department of the Environment, Water, Heritage and the Arts
Department of the Prime Minister and Cabinet
Equal Opportunity for Women in the Workplace Agency
Family Court of Australia
Federal Court of Australia
Food Standards Australia New Zealand
Future Fund Management Agency
Great Barrier Reef Marine Park Authority
Indigenous Business Australia
Insolvency and Trustee Service Australia
IP Australia
Medicare Australia
Migration Review Tribunal and Refugee Review Tribunal
National Archives of Australia
National Blood Authority
National Competition Council
National Environment Protection Council
National Film and Sound Archive
National Health and Medical Research Council
National Library of Australia
National Museum of Australia
National Offshore Petroleum Safety Authority
National Water Commission
Native Title Tribunal
Office of National Assessments
Office of the Commonwealth Director of Public Prosecutions
Office of the Commonwealth Ombudsman
Office of the Inspector General of Taxation
Office of the Privacy Commissioner
Private Health Insurance Ombudsman
Productivity Commission
Professional Services Review
Royal Australian Mint
Social Security Appeals Tribunal
Special Broadcasting Service Corporation (SBS)



Superannuation Complaints Tribunal
Torres Strait Regional Authority
Tourism Australia
Wheat Exports Australia
Workplace Authority

