Attorney-General's Department Website

Privacy Impact Assessment

Attorney-General's Department

29 January 2013

ERNST & YOUNG

ERNST & YOUNG

121 Marcus Clarke Street
Canberra ACT 2600 Australia
GPO Box 281 Canberra ACT 2601
Tel: +61 2 6267 3888
Fax: +61 2 6246 1500
www.ey.com/au

Ms S22(1)
Project Manager
Attorney-General's Department
Email: S22(1) @ag.gov.au

29 January 2013

Private and confidential

Privacy Impact Assessment – Attorney-General's Department Website

Dear S22(1),

Thank you for providing Ernst & Young with the opportunity to conduct a Privacy Impact Assessment (PIA) of the redevelopment of the Attorney-General's Department (the Department) website, www.ag.gov.au. The website is a key communication mechanism for the Department and represents a major investment for the Department. The PIA has focused on the new website managed under the domain name www.ag.gov.au. The Department's internal networks and other domain names were excluded from this PIA.

The PIA identified an issue related to the capture of private information for the training courses operated by the Department's Protective Security Training Centre. As at the date of this report, the pages collecting personally identifiable information were still configured to transmit the collected information in clear text.

The attached report details the findings and recommendations from the PIA and includes as appendices the Threshold assessment and the Privacy Impact Assessment Checklist.

We would like to take this opportunity to thank all of the participants of this PIA for their cooperation and timely provision of information.

Should you have any queries relating to this internal audit, please contact Paul Kastner (Client Engagement Partner) on (02) 9248 4880.

Yours sincerely

Paul Kastner
Partner
Ernst & Young

Attachment: Privacy Impact Assessment Report

Contents

1. Executive Summary

The Attorney-General's Department (the Department) has embarked on a project to redevelop its Internet website (www.ag.gov.au) which has included fundamental changes to the infrastructure and technology hosting the environment. The magnitude of change to the information flows within the environment warranted a Privacy Impact Assessment (PIA) to be conducted over the redeveloped website.

The scope of the PIA was limited to the Department's redeveloped website, which will operate on two load balanced servers supported by an administration server and a Microsoft SharePoint 2010 database. Specifically excluded from the scope of the PIA are the servers and information used to support the Department's internal network and other external facing domains not operating under the www.ag.gov.au domain.

Our approach to conduct the PIA was to:

1. Develop the project description by broadly describing the project, including the aims and whether any personal information would be handled

2. Map information flows and the privacy framework by describing and capturing information flows relevant to personally identifiable information.

3. Identify and analyse the privacy impacts of the project.

4. Advise on privacy management by developing a process to manage privacy impacts.

From our procedures we noted that the website (and the associated external facing web servers) do not contain personally identifiable information, nor is there an intent that the website contain personally identifiable information. The Department has established processes to review information before it is posted to the Department's website, including steps to seek advice from the Department's Privacy Officer. It was however observed that there are mechanisms in place on the website that collect information, some of which is personally identifiable information.

The PIA identified that the Department collects information from individuals through the website via four methods:

- Forms (general enquiry, media enquiry, training registration and recognition of prior training);
- Cookies;
- Logged information; and
- Google Analytics.

Of these four methods, the Protective Security Training Centre (PSTC) registration form was identified as collecting personal identifiable information. The information collected is required to register individuals for training at the PSTC, as the PSTC is a Registered Training Organisation. The information is collected and transmitted to the Department's internal email system in clear text. It is recommended that forms used to collect personally identifiable information from users through the Department's website (including the Protective Security Training Centre (PSTC) registration form) use Hyper Text Transfer Protocol Secure Socket Layer (HTTPS) to encrypt the website session with a digital certificate to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse to the personally identifiable information collected within the form.

We further recommend that the Department also consider:

- Conduct future PIAs earlier in the project to permit adequate time for the Department to action recommendations;

- To make the notices relating to the collection of information more explicit, including advising users registering for courses offered through the PSTC, reflecting the legislative requirement to collect the personally identifiable information;
- To increase the awareness of the role of the Department's Privacy Officer so that branches seek guidance from the Department's Privacy Officer when considering placing information on the website that is potentially personally identifiable information; and
- Conduct a PIA on the end-to-end flow of personally identifiable information collected for the purposes of the PSTC to confirm that the privacy principles are applied to the information collected by the PSTC.

2. Introduction

The Department has been conducting a project to redevelop its primary website (www.ag.gov.au) to address known website management issues. This project will introduce new technologies to make the management of the website more efficient.

By delivering a redeveloped website based on the Department's Microsoft SharePoint 2010 Platform. Content from the existing Department website will be assessed, reviewed, migrated and updated or archived (as determined by the project team). The project will not change content or create new websites under other domain names.

In order to assess the privacy impact requirements of the new website Ernst & Young was engaged to conduct a PIA.

2.1 Objective and scope

The objective of this PIA is to understand the information flows of information within the Department's website as governed by the Privacy Act of 1988.

The Department has requested a PIA of the Department's Website Redevelopment Project in accordance with the Office of the Privacy Commissioner's PIA Guidelines 2012. The PIA deliverable is a report of findings and recommendations.

The scope of the PIA is limited to the Department's new website, which will operate on two load balanced servers supported by an administration server and a Microsoft SharePoint 2010 database. Specifically excluded from the scope of the Privacy Impact Assessment are the servers and information used to support the Department's internal network and other external facing domains. The diagram below indicates the environment in scope for this PIA. Appendix C – Scope statement includes a detailed copy of the scope.

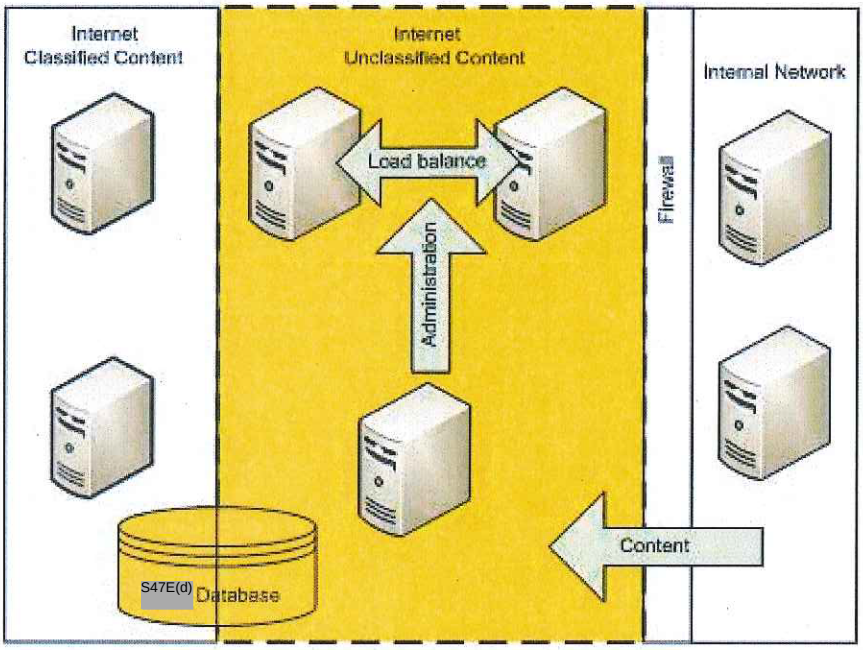

Figure 1 - the Department's Website Redevelopment Project Environment

2.2 Approach

Ernst & Young's approach to delivering the PIA is aligned to whole of government guidelines issued by the Office of the Privacy Commissioner and considered key online privacy risks. The approach included four key phases, outlined below. A diagram showing the approach is found in Appendix D – PIA approach:

2.2.1 Project description

This phase broadly described the project, including the aims and whether any personal information was being handled. The outcomes from this phase included a description of the project, covering:

- Overall aims;
- Alignment of the project's privacy aims with the Department's broader privacy objectives;
- The scope and extent of the project; and
- The existing links with other projects and or programs and the key privacy elements.

During this phase, in order to assess the privacy impact requirements of the new website a Threshold Assessment was conducted; see Appendix A Threshold Assessment.

2.2.2 Mapping information flows and privacy framework

A preliminary assessment of the privacy impact was undertaken during this phase following an information flow map which described and mapped the project's personal information flows including:

- Handling, collection and usage processes of personal information;
- Internal flows of information, disclosures, security and data quality measures,
- Privacy, secrecy or legislation applying to information flow,
- Organisational business or privacy rules applying to information flow; and
- Mapping the current personal information environment and possible effects.

An information flow map was produced based on the above mapping conducted as illustrated in Appendix F Information flows.

2.2.3 Privacy impact analysis

A privacy impact analysis was conducted during this phase of the PIA in order to identify and analyse the project's privacy impact. The privacy impact analysis included:

- Identification of the privacy and necessity of impacts;
- The impact on project goals;
- Evaluation of the information collected from the website;
- Analysis of privacy outcomes, and/or unacceptable privacy impacts;
- Handling of privacy breaches;
- Compliance with relevant privacy legislation;
- Existence of audit and oversight mechanisms; and
- Estimating the value of private information being collected.

Measuring the handling of private information during this phase for compliance against relevant Government Information Privacy Principles (IPPs) was also undertaken. The IPP Checklist was completed and is found in Appendix B – Information Privacy Principles Checklist.

2.2.4 Privacy management

The final phase was to develop a process for managing privacy impact. This involved developing responses with the Department's stakeholders in order to lessen the identified privacy impacts.

To conduct the procedures outlined above interviews were conducted with key stakeholders. The listing of personnel interviewed as part of this PIA is found in Appendix G – Personnel contacted in this PIA. Documentation was provided as part of the interviews and assessment of the documentation formed part of the analysis in the PIA. The listing of documentation and material accessed during this PIA is found in Appendix H – Reference sources for the PIA.

3. Privacy Impact Assessment

3.1 Project description

We noted that the Department's redeveloped website is not intended to store personally identifiable information or to be an access portal for users of the website to access personally identifiable information. The primary function of the Department's website (www.ag.gov.au) is to provide information to the public (in Australia and overseas) and to provide a mechanism for the Department to communicate information relating to the Department's six strategic priorities.

The scope of the project is limited to redevelopment of the Department's Internet website (www.ag.gov.au). The project introduced Microsoft SharePoint 2010 operating on two load balanced web servers with an administrative server and a Microsoft SharePoint 2010 database. The project will not change content or create new websites under other domain names.

The website is not intended to store or disclose personally identifiable information, which is aligned with the Department's privacy objectives of not disclosing private information relating to employees, citizens and other people.

3.2 Mapping information flow and privacy framework

We found that control mechanisms are in place to review the flow of information from the Department's internal network out onto the website. A process is in place for owners of information on the website (branch managers) to request updates to the website and to prepare revisions of the information. The control mechanisms include review and approval of the changes by the branch head, before the changes are submitted to the web development team, which then seeks approval of the changes by the Departments Strategic Communications team prior to the changes being deployed to the web pages. See Appendix F – Information flows Diagram 1 – Content deployment, for a diagrammatic overview of the process to request information to be changed on the website. It was noted that the process described operates the same for both normal changes and emergency changes to the web site. This change process was not tested as part of this PIA.

We found that the Department has a Privacy Officer, who is responsible for providing guidance to the Department on privacy matters, including requests to place potentially personally identifiable information on the Department's website.

Based on consultation with the network operations team and the Department's information technology security advisor we determined that the external facing network is separated from the internal network, with the purpose of restricting access to make changes to the external facing environment. Access is limited to key individuals to make changes to the website content. The network operations team and the information technology security advisor described the security monitoring controls operating around the web server environment.

We found that the website includes various disclosures including disclosures relating to privacy, confidentiality and freedom of information.

3.3 Privacy impact analysis

We identified that the Department collects information through four methods:

- Forms (general enquiry, media enquiry, training registration and recognition of prior training). These forms are currently operating in clear text on the existing Department website with information transmitted in clear text. See Section 4.1 Protective Security Training Centre information collection for more information.

- Cookies. The website utilises session cookies to allow users improved experience while accessing the Department's website. The cookies expire upon closure of the website by the user. The Department does not access these cookies.

- Logged information. The website logs browser and operating system version; referring site address; IP address of the user; the date and time of visit; the address of pages accessed; and

the documents downloaded. The information is used for statistical analysis and systems administration purposes. It does not identify individuals and is protected with the same security mechanisms as the Department applies to its external facing servers. The information is only disclosed in the case of investigation by a law enforcement agency. This information is not covered by the Act.

- Google Analytics. The Department uses Google Analytics to understand the way people use the Department's website. Information is collected relating to the pages are visited; and the IP address of the user. This information is stored on US servers, and is used and disclosed as per Google's Privacy Policy. The information collected is not covered by the Act.

3.4 Privacy management

We consulted with the SharePoint development team and the Director, PSTC to discuss options to protect personally identifiable information entered from the PSTC web pages. It was determined that an appropriate mechanism to protect the personally identifiable information from point of data entry to the point of entry into the Department's internal network, is to encrypt the PSTC web pages using SSL encryption.

Detailed discussion of the observation and recommendation relating to the PSTC web pages are found in Section 4 – Detailed observations and recommendations.

4. Detailed observations and recommendations

4.1 Protective Security Training Centre information collection

As a service to appropriately employed individuals and the Australian Government, the Department offers training in protective security through the Department's Registered Training Organisation (RTO), the Protective Security Training Centre (PSTC). The PSTC provides training in protective security, personnel security (vetting), security risk management, government investigations, physical security and information and communications technology security.

We noted that the Department collects individuals' personally identifiable information when individuals register to participate in training offered by the PSTC. The information gathered includes:

- Personal information (name, date of birth, address, telephone and email contact details, country of birth, and Aboriginal / Torres Strait Islander background);
- Health information (disabilities, special dietary requirements);
- Education information (highest qualification, year completing school); and
- Employment information (employer, supervisor details, work contact information).

The same section of the Department's website also has a form to recognise prior training. The form requests the same information as the registration form with some additional information relating to the reason for seeking recognition.

A user registering for the course (or for recognition of prior training) is required to accept the privacy statement on the page.

The information is then transmitted to the PTSC through Simple Mail Transfer Protocol (SMTP) and received into the Department's internal mail system (see Diagram 2 – Web form information transfer in Appendix F – Information flows). Based on consultation with the web team and the network operations team we understand that a copy of the information is not stored on the server. Once the information is transmitted to the internal mail server the information is outside the scope of this PIA.

We observed that web pages for both the registration and the prior training recognition forms are in clear text and that the proposed new website was intended to collect the information in clear text. As at the writing of this report the web pages for both forms were operating in http, which means that information transmitted from the webpage to the server is transmitted in clear text.

4.1.1 Risk

There is a risk that people registering to attend training courses offered through the Protective Security Training Centre may have their private information accessed by unauthorised individuals. This could include persons intercepting packets transmitted to the Department or third party users monitoring the Department's Internet Gateway.

Using the Department's risk rating scale (see Appendix E – Attorney-General's Department risk ratings) the risk is evaluated as medium. Application of the recommendation below should move the risk rating to very low.

4.1.2 Recommendation

We recommend that the Department updates the new website to require that the web pages on which individuals register for training or seek recognition of prior training, be secured to https using SSL encryption. This will encrypt the information from the point that the information is transmitted from the end user's computer to the server on which the information is recorded. It is further recommended that for all future pages where the Department is capturing personally identifiable information, those pages are secured to https with SSL certificates applied to encrypt the information during transmission.

It is also recommended that for the PSTC web pages, that the Department should clearly inform its users of the reason and purpose for the collection of personal information, and the legislative instrument requiring the PSTC to collect the information.

4.2 Other observations and recommendations

The following observations and related recommendations were made throughout the assessment of the privacy impact, and while these do not necessarily impact the overall assessment, we recommend they be considered in future projects:

4.2.1 Timing of the Privacy Impact Assessment

The timing of the Privacy Impact Assessment was late in the project and this report was only finalised after the website had been moved into the production environment. It is recommended that for future projects the Department consider conducting the Privacy Impact Assessment earlier in the project alongside the threat and risk assessment and / or the attack and penetration testing of the website and application.

4.2.2 Privacy notices

Specifically with respect to the pages used by the PSTC to register for training and recognise prior training, the Department should clearly inform its users of the reason and purpose for the collection of personal information, and the legislative instrument requiring the PSTC to collect the information. The notices should include information on the means by which an individual can amend personal information submitted on the forms should they realise that information submitted was incorrect.

4.2.3 Awareness of the role of the Privacy Officer

While branch managers may be aware of the role of the Department's Privacy Officer, it is recommended that the Department take steps to increase the awareness of the role and services that it can provide to assist personnel who are considering activities which could involve personally identifiable information.

4.2.4 Detailed PIA of PSTC information flow

The retention and use of the information collected by the PSTC was outside the scope of this PIA. However, we recommend that the Department consider conducting an end to end PIA to confirm that privacy principles are applied across the lifecycle of the information collected via the website.

5. Management Responses

5.1 Protective Security Training Centre information collection

Recommendation on implementing HTTPS to protect personally identifiable information submitted via forms is acknowledged. Since the report was prepared, webpages collecting personally identifiable information have had https implemented.

The recommendation regarding the timing of PIAs will be built into project procedures and shared the department's Project Management Office.

The recommendations not directly impacting the project will be shared with the appropriate staff.

5.1.1 Owner: S22(1)

5.1.2 Action date: Complete

Appendix A Threshold Assessment

Organisation
This Threshold Assessment has been completed for the Attorney-General's Department (the Department).

Contact
Ernst & Young
121 Marcus Clarke St,
Canberra ACT 2600, Australia
Office: +61 2 6267 3888
Fax: +61 2 6246 1500

Project Description
The Department is remodelling its primary website (www.ag.gov.au) in order to address known website management issues. This project does not change or create new websites under other domain names.

The project objective is to deliver a redeveloped website based on the Department's Microsoft SharePoint 2010 Platform. Content from the existing Department website will be assessed, reviewed, migrated and updated or archived (as determined by the project team).

The project manager for the project is S22(1) .

In order to assess the privacy impact requirements of the new website this Threshold Assessment has been conducted to address the need for a Privacy Impact Assessment (PIA).

Collection, Use and Disclosure of Personal Information
The Department collects information through four methods: forms, cookies, logged information and Google Analytics. Collection, use and disclosure of personally identifiable information, by the Department, is subject to the Privacy Act 1988 (the Act) which requires that the Department comply with the Information Privacy Principles (IPPs) set out in the Act. The Department also operates in accordance with the Guidelines for Federal and ACT Government World Wide Websites issued by the Office of the Privacy Commissioner.

The website in development for the Department is intended to replace the Department's current website. The new website will collect data in the same mechanism using the same forms, for the same use and covered by the same disclosures as the current website. The difference between the current website and the new website is 'look and feel' only.

Forms
The Department collects information from website users on four separate forms. These are:

- Media contact form – no personally identifiable information requested, however, such information could be entered by the user completing the form.
- General Enquiry form - no personal identifiable information requested, however, such information could be entered by the user completing the form.
- Feedback and Complaints form – no personally identifiable information requested, however, such information could be entered by the user completing the form.
- Protective Security Training Centre (PSTC) registration form – personal identifiable information is collected. This information relates is required to register individuals for training at Registered Training Organisations.
- PSTC Previous Experience Recognition form – personal identifiable information is collected. This information is required to register individuals for training at Registered Training Organisations and recognise previous experience and training.

The information collected on the PSTC forms are:

- Personal information (name, date of birth, address, telephone and email contact details, country of birth and Aboriginal / Torres Strait Islander background);
- Health information (disabilities, special dietary requirements);
- Education information (highest qualification, year completing school); and
- Employment information (employer, supervisor details, work contact information).

As per the Department's Identifying Personal Information policy, this information is used for course administration, statistical analysis, evaluation of programs, and to deliver information about future courses and events. Course administration details may be disclosed to employers if a written request is sent to the PSTC.

The PSTC registration form contains a Confidentiality Policy outlining that all information provided during assessment in either electronic or hardcopy format is official government information under the provisions of the Crimes Act 1914 (sections 70 and 79) and is issued on a need-to-know basis. The information will be stored, transmitted and disposed of in accordance with the Protective Security Policy Framework (PSPF) Information Security Management Guidelines.

The information is collected by the webpage and transmitted by simple mail transfer protocol (SMTP) to the PSTC. Per representation by the SharePoint development team and the IT Operations team, the email is generated (and not stored) in the user session and transmitted to the email content filter (MailMarshall). Once the data is transferred to the PSTC the information is no longer in the scope of this PIA. Retention of this information by the PSTC, recording of the data into the PSTC training application, and use of the information by the PSTC is outside the scope of this privacy impact and has not been considered.

At the time of the PIA, the web pages on which the data is collected were unsecured Hyper Text Transfer Protocol (http) pages. It is recommended that they be updated to be Hyper Text Transfer Protocol Secure (https) using secure-socket-layer (SSL) 128bit encryption, thus encrypting the data from the point of transmission from the web-browser to the web server.

Logged information
When visiting the Department's website, the following information is logged per individual:

- Browser and operating system;
- Top level domain name (.com, .gov, .au, etc.);
- Referring site address;
- IP address;
- Date and time of visit; and
- Address of pages accessed and the documents downloaded.

This information is used for statistical analysis and systems administration purposes, and not to identify individuals. It is only disclosed in the case of investigation by a law enforcement agency. This information is not covered by the Act.

Cookies
When visiting the Department's website, the Department's server generates a session cookie which is used to keep track of pages accessed by the user while using the Departments server. The cookie allows the user to navigate back and forwards through the web site and return to pages previously visited. The cookie exists only for the time the user is accessing the Department's server. The information collected is not covered by the Act.

Google Analytics
Through the use of Google Analytics, the following information is collected by Google:

- Web pages accessed during the session; and
- IP address of the user.

This information is stored on US servers, and is used and disclosed as set out by Google's Privacy Policy. The information collected is not covered by the Act.

Assessment Finding

As the new website will collect personal and sensitive information under certain circumstances the Threshold Assessment concludes that a Privacy Impact Assessment needs to be completed.

Name	Name
_____	_____
Signature	Signature
_____	_____
(Proponent)	*(Proponent)*
Date	Date
_____	_____

Appendix B Information Privacy Principles Checklist

IPP 1 – Manner and purpose of collection

IPP 1
The information must be necessary for the agency\'s work, and collected fairly and lawfully.

---

1. Is the information collected for a lawful purpose directly related to a function or activity of the collector?

   Yes.

   Personal information is collected for the purposes of course administration, statistical analysis and evaluation of the Department's programs in accordance with the Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) Data Element Definitions: Edition 2.1 which provides a nationally consistent framework for the collection of vocational education and training (VET) information.

   Personally identifiable information is not displayed on the website or stored on the website servers.

2. Will the information collected be necessary for or directly related to that purpose?

   Yes.

   The information collected is for the Protective Security Training Centre (PSTC) to accommodate the needs and / or requirements of its clients undertaking the Protective Security Training course.

3. Will the information be collected by lawful and fair means?

   Yes.

   The information collected from the Protective Security Training Centre (PSTC) registration form is collected directly from the participant applying for the course. The information requested is information that must be collected by Registered Training Organisations under the requirements of the AVETMISS.

IPP 2 – Solicitation of personal information from individual concerned

---

IPP 2
An agency must take steps (usually through an IPP 2 notice) to tell individuals:

- why they are collecting personal information
- what laws give them authority to collect it
- who they usually disclose it to

---

1. Is the collector soliciting the personal information from the individual concerned?

   Yes.

   The personally identifiable information is solicited through the Department's website (www.ag.gov.au).

2. Will reasonable steps be taken to tell the individual about the purpose of the collection?

   Yes.

   The Department's website (www.ag.gov.au) provides an Identifying Personal Information Policy on the Protective Security Training Centre (PSTC) registration form. However, more clarity needs to be given to the users regarding why certain information is being collected, i.e. health care identifiers used for accommodating special requirements during the training course.

3. If the collection is authorised or required by law, will the individual be advised?

   Yes.

   The Department's website (www.ag.gov.au) provides an Identifying Personal Information Policy on the Protective Security Training Centre (PSTC) registration form. Personally identifiable information is collected for the purposes of course administration, statistical analysis and evaluation of the Department's programs in accordance with the Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) Data element definitions: Edition 2.1. Users are advised that the information is required to register for the website, however, further clarity could be provided to allow users to understand the legislative requirements for collection of the information.

4. Will the individual be advised about the usual disclosures?

   Yes.

   The PSTC page includes three disclosures, the first relating to course cancellation; the second relating to personal identifiable information and the third relating to confidentiality. The disclosure statements are below.

   > Cancellation Policy: If you are unable to attend, we would welcome a substitute participant. An invoice may be issued three weeks prior to the course commencement date and you will be liable for the course fees. So as to not incur the course fees, a written cancellation must therefore be received by the Protective Security Training Centre (PSTC) at least three weeks prior to the course commencement date. In the case of non-attendance due to illness, participants may reschedule to a later program at no charge but only if a medical certificate is provided to the Director of the PSTC. If the PSTC cancels a course, participants will be offered a rescheduled course or a full refund. The PSTC reserves the right to cancel, postpone or reschedule a course.
   >
   > Identifying Personal Information: We collect your personal information for the purposes of course administration, statistical analysis and evaluation of our programs. Some course administration details may be disclosed to your employer for administration and statistical/monitoring purposes if they make a written request to the PSTC. Your information will not be used for any other purpose except as required or authorised by or under law. Your information may be used to inform you about other Protective Security Training Centre courses or sponsored events.
   >
   > Confidentiality Policy: All information provided during assessment in either electronic or hardcopy format is official government information under the provisions of the Crimes Act 1914 (sections 70 and 79) and is issued on a need-to-know basis. It will be stored, transmitted and disposed of in accordance with the Protective Security Policy Framework (PSPF) Information Security Management Guidelines.

   Users completing the Protective Security Training Centre (PSTC) registration form are provided with an additional check box to advise the Protective Security Training Centre (PSTC) of whether they wish to have their personal information used for marketing purposes.

IPP 3 – Solicitation of personal information generally

IPP 3

An agency must take reasonable steps to ensure the personal information it collects is:

- relevant
- up-to-date and complete
- not collected in an unreasonably intrusive way

---

1. Will reasonable steps be taken to ensure that any solicited personal information collected is relevant, up to date and complete?

   Yes.

   The user completing the registration form ensures information entered into the Protective Security Training Centre (PSTC) registration form is relevant, up to date and complete.

2. Will reasonable steps be taken to ensure that the information will be collected in a way that does not unreasonably intrude on the individual?

   Yes.

   The information collected for the Protective Security Training course is collected for the purposes of course administration, statistical analysis and evaluation of the Department's programs in accordance with the Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) Data Element Definitions: Edition 2.1

IPP 4 – Storage and security of personal information

IPP 4
Personal information must be stored securely to prevent its loss or misuse.
If you want to modify information technology (IT), you may also have to manage other agency-specific processes. Include a summary or copy of the process in the PIA record.

Note: The unit responsible for IT maintenance and security should complete any assessments about new or existing systems. The unit manager should sign off on the assessment.

---

a) Security safeguards

1. Will there be reasonable technical security in place to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse?

   Yes, however, as at the date of this report, SSL certificates required to encrypt the data had not been applied to the website.

   The Protective Security Training Centre (PSTC) registration form should use Hyper Text Transfer Protocol Secure (HTTPS) which encrypts the website session with a digital certificate to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse while the information is in transit from the user's computer to the web server. The information will not reside or be stored on the web server.

2. Will there be reasonable physical security in place to protect against loss, unauthorised access, use, modification or disclosure and other misuse?

   Yes.

   The Department's servers are housed at the Attorney-General's Data Centre in Symonston to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse. Based on consultation we understand the web servers to be based as Symonston.

3. Will there be security policies and procedures in place during the handling (routine or otherwise) of the information?

Yes.

Security policies exist within the Department to address information security. This includes Security Risk Management Plans and System Security Plans.

4. Will controls and procedures be created for the authority to add, change or delete personal information?

   Not Applicable. The personally identifiable information obtained from the PSTC is not stored on the web servers. It is transmitted in the form of an email via SMTP to the PSTC inbox on the Department's internal email server. The internal network, including the Microsoft Exchange server, and accounts used to collect this information are outside the scope of this PIA.

5. Will system security include an ongoing audit process to track system use, including back-up materials?

   Not Applicable. The personally identifiable information obtained from the PSTC is not stored on the web servers. It is transmitted in the form of an email via SMTP to the PSTC inbox on the Department's internal email server. The internal network, including the Microsoft Exchange server, and accounts used to collect this information are outside the scope of this PIA.

6. Will audit mechanisms identify inappropriate system access?

   Yes.

   Based on consultation with the Network Operations team and the information technology security advisory security monitoring is in place through the Department's Network Operations team and the Security Operations team. However, as noted previously, personally identifiable information obtained from the PSTC is not stored on the web server.

b) Safeguarding information provided to external parties

An agency must take reasonable steps to prevent the unauthorised use or disclosure of information it gives external parties providing a service to the agency (such as private sector contractors, overseas agencies or organisations).

1. Will the contractual obligation the agency imposes on the external party comply with s 95B of the Privacy Act?[20]

   The PSTC does not engage third parties to manage the information.

   A third party, Verizon, manages the Internet Gateway for the Department. It is intended that the web pages will be secured using SSL and therefore the information would not be visible to Verizon. As at the date of the report, the SSL certificates had not been applied. A copy of the contract between the Department and Verizon was requested however was not yet available.

   It is expected that the web pages used to collect the information will be protected using SSL encryption and as such the Department's third party provider of internet gateway (Verizon) will not be able to access the information when it is transmitted across the gateway as it will be encrypted.

2. Will the contract include requirements inconsistent with NPPs 7-10?

   As noted above, the information will be encrypted using SSL, however, web pages were not using SSL as at the date of the report. A copy of the contract between the Department and Verizon was requested however was not yet available.

3. Will the agreement with a State/Territory government or agency/body or the arrangement with a foreign government, agency, body or organisation include:

   - Explicit undertakings that the recipient will afford the same privacy restrictions and protections as the information received in the hands of the Commonwealth agency. (This includes against different third party uses and disclosures.)

Note: Also consider IPP 11.3 obligations (see below) at this point.

Not Applicable. The website does not rely on any agreements with state governments, foreign government agencies or bodies.

IPP 5 – Information related to records kept by a record-keeper

---

IPP 5

A record-keeper must take reasonable steps to allow a person to find out:

- if the record-keeper has possession or control of personal information
- the nature of that information
- the purposes that information is used for
- the steps to take to get access to their record

The record-keeper must maintain a record of the:

- nature of records kept
- purpose of each type of record
- classes of individual about whom records are kept
- period each type of record is kept
- persons that may have access to the records and when
- how an individual can access their records

The record-keeper must make sure that:

- this information is made available for public inspection
- a copy of this record is given to the Privacy Commissioner in June each year

---

1. Will the record-keeper be authorised by law to refuse to inform any person of the records in the record-keeper's possession or control?

   Not Applicable. Records the personally identifiable information will not be maintained within the environment which was the scope of this PIA.

2. Will processes be put in place to satisfy obligations at question 1 above?

   Not Applicable. As noted above personally identifiable information will not be maintained within the environment which was the scope of this PIA.

IPP 6 – Access

IPP 6

Individuals can have access to records, unless the record-keeper is required or authorised to refuse access under any Commonwealth law.

(This IPP effectively grants access to information on the basis of the rights available under the Freedom of Information Act 1982.)

---

1. Will processes be put in place to provide access to records under the relevant Commonwealth law such as the Freedom of Information Act 1982 or the Archives Act 1901?

   Not Applicable. As noted in IPP5 personally identifiable information will not be maintained within the environment which was the scope of this Privacy Impact Assessment. Should individuals want to access records collected through the website, then other policies and procedures governing the Department's internal networks will be applicable. These other policies, procedures and technologies were not the subject of this PIA.