



# FSA Privacy Impact Assessment and Privacy Notice for Websites



## Introduction

The E-Government Act of 2002 is a new mandate to maintain/increase the integrity with which public information is handled by the government. Section 208 requires FSA to complete a Privacy Impact Assessment for each system that collects information in identifiable form about the general public.

During the Definition Phase of the FSA Solution Lifecycle, the SSO must ensure that the team completes the attached Privacy Impact Assessment Questionnaire and must file the completed form in the system's Security Notebook as part of the system's documentation. The electronic copy of the completed form should be stored in the system's Security Folder.

## Timing

A PIA (or amendment of a PIA) is required in the following circumstances related to information in identifiable form:<sup>1</sup>

- a. Conversions -- when converting paper-based records to electronic systems;
- b. Anonymous to Non-Anonymous -- when functions applied to an existing information collection change anonymous information into information in identifiable form;
- c. Significant Management Changes -- when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- d. Significant Merging -- when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated<sup>2</sup>;
- e. New Public Access -- when user-authenticating technology (e.g., password, digital certificate) is newly applied to an electronic information system accessed by members of the public;
- f. Commercial Sources -- when agencies incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources (merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- g. New Uses -- when agencies work together on shared functions involving new uses or exchanges of information in identifiable form, such as the

---

<sup>1</sup> In addition, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs on existing electronic information systems as s/he determines appropriate.

<sup>2</sup> No PIA is required when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act.



# FSA Privacy Impact Assessment and Privacy Notice for Websites



cross-cutting e-government initiatives; in such cases, the lead agency should spearhead the PIA activity.

Agencies must update or revise a completed PIA when there has been a significant change in the collection or flow of data, e.g., new uses or disclosures of information, incorporation into the system of additional items of information in identifiable form, etc.

## **Large Systems**

For systems that are considered large, agencies must conduct more extensive analyses of (i) the consequences of collection and flow of information, (ii) the alternatives to collection and handling as designed, (iii) the appropriate measures to mitigate risks identified for each alternative and (iv) the rationale for the final design choice or business process.

Large systems are systems or projects that require special management attention because of its:

- its importance to an agency mission,
- high cost of development, operation or maintenance,
- is a financial management system that costs more than \$500,000,
- is directly tied to the top two layers of the Federal Enterprise Architecture (Services to Citizens and Mode of Delivery),
- is an integral part of the agency's modernization blueprint (i.e., enterprise architecture),
- is defined as major by the agency's capital planning and investment process,
- has significant program or policy implications,
- has high executive visibility, or
- is E-Government in nature or uses e-business technologies.

## **Privacy Notices for Websites**

In addition to the Privacy Impact Assessment, the E-Government Act of 2002 also mandates that Privacy Notices must be placed on agency websites; including the principal web site and pages where substantial information in identifiable form is collected. The web page author must include or hyperlink to a Privacy Notice on any form or page where a user enters personal information. Most of the content of the Privacy Notice comes from responses to the Privacy Impact Assessment Questionnaire. Specifically, the Notice must include:

- What information is being collected;
- Why the information is being collected;
- The intended use of the information;
- With whom (ex. Other agencies) the information will be shared (if at all);



## FSA Privacy Impact Assessment and Privacy Notice for Websites



- What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- How the information will be secured; and
- The rights of the individual under the Privacy Act and other laws relevant to protection of the privacy of an individual. (This section could include the following, “If you have any additional questions regarding your Privacy Act rights as related to the information we collect, please contact email *address of SSO or someone in Dept of Ed*. The complete description of Department of Education online privacy policies can be located at the Department of Education homepage, <http://www.ed.gov/utilities/privacy.jsp>.”)



# FSA Privacy Impact Assessment and Privacy Notice for Websites



## Privacy Impact Assessment Questionnaire

System Name:

System Owner:

Privacy Impact Assessment Questionnaire Author:

Date:

1. What information will be collected for the system (Ex. Name, Social Security Number, annual income, etc)?
2. Why is this information being collected?
3. How will FSA use this information?
4. Will this information be shared with any other agency? If so, with which agency or agencies?
5. Describe the notice or opportunities for consent would be/ or are provided to individuals about what information is collected and how that information is shared with others organizations. (e.g., posted Privacy Notice)
6. How will the information be secured? (An overview of security controls described in the system security plan (Technical Controls section) would be applicable to answer this question.)
7. Is a system of records being created or updated with the collection of this information? (A system of record is created when information can be retrieved from the system by the name of the individual or an identifying number, symbol or other identifying particular assigned to an individual. Also, in responding to this question a helpful reference may be to the system's System of Record organization step completed in the Definition phase of the Solution Lifecycle process.)
8. List the web addresses (known or planned) that will have a Privacy Notice.