AINS, INC.

OFFICE OF THE COMPTROLLER OF THE CURRENCY

APPENDIX F: PRIVACY IMPACT ASSESSMENT - FOIAXPRESS

Date: September 28, 2012

Office of the Comptroller of the Currency

Prepared by: AINS
Version: 0.1

Table of Contents

Revision History

Version Number	Release Date	Summary of Changes	Section Number / Paragraph Number	Changes Made By
0.1	09/28/2012	Final	All	AINS
.				

Abstract

AINS Inc. (AINS) was awarded the opportunity to implement the FOIAXpress (FX) and Public Access Link (PAL) systems for the Department of the Treasury – Office of the Comptroller of the Currency (Treas. OCC) as the solution for their Freedom of Information Act (FOIA) / Privacy Act (PA) tracking system, which is used in response to FOIA/PA requests from the public. FX and PAL provides the FOIA office with a centralized system to handle and track request/appeal submissions, electronically redact responsive documents, and compute statistics for the FOIA Annual Report, per the Department of Justice's (DOJ) requirements.

Overview

OCC's e-FOIA system is a web-based system that will electronically process FOIA, PA, and appeal requests. The system configuration coupled with the software and hardware information provides the OCC with the ability to effectively automate the FOIA business process from receipt of the request through delivery of responsive documents.

FOIAXpress (FX) is the most comprehensive, web-based, Commercial Off The Shelf (COTS) application available for processing FOIA and PA requests. It is currently utilized by over 100 government agencies and is recognized as the best value solution. FX electronically creates requests, stores requester details, and redacts responsive documents for delivery to requesters. It also tracks FOIA processing statistics/fees and generates reports on the number/types/disposition of requests, as required by the U.S. Department of Justice (DOJ). Additionally, with the optional implementation of the Public Access Link (PAL) to FX, requesters may create and track their submissions online.

The deployment of FX has provided compliance with the e-FOIA regulations and has transformed the request management experience from a very manual task to an efficient automated business process. In addition to the many features that this robust application provides, at a minimum, the FX system has facilitated a centralized application allowing users to create a request and stores requester details, assign a request for processing to an individual or group of users and transfer a request to the proper action office, send correspondence through the use of templates with insert fields for letters such as the initial acknowledgement and final response, perfect a request and identify the multi-track type, submit a request for documents to retrieve the requested information, add responsive records and perform redactions, apply estimated costs and generate invoices, confirm the exemption codes applied and final disposition, quickly close/amend a request, and easily generate numerous types of reports, including the FOIA Annual Report with all the requirements per DOJ.

1 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Types of information in the records include requesters' and their attorneys' or representatives' names, addresses, e-mail, telephone numbers, and FOIA case numbers; office telephone numbers, and office routing symbols of OCC employees and contractors; names, telephone numbers, and addresses of the

submitter of the information requested; unique case identifier; social security number (if provided by the requesting party).

- Requester details
  - Requester's name (First Name*, Middle Name, Last Name*)
  - Requester's organization
  - Requester's category* (e.g. Commercial Use, Educational Institution, News Media, Non-commercial Scientific Institution, Other
  - Requester's address (Street, City, State, Zip, Country*)
  - Requester's phone numbers (home, work, mobile, fax)
  - Requester's email
- Request details
  - Requester's name (First Name*, Last Name*)
  - Shipping address (Street, City, State, Zip, Country*)
  - Other address (Street, City, State, Zip, Country)-if different from shipping address
  - Billing address (Street, City, State, Zip, Country)-if different from shipping address
  - Request description (e.g. what the requester is asking for in their FOIA/PA request)
  - If fees/invoices and payment applies to a request, then the system may track the 'amount due', 'check#', 'bank name', credit card details('card type', 'card#', 'name on card', 'expiration month'

Additionally, FOIAXpress stores 'files' within the correspondence log for a request AND within the document management module (for responsive records), which may include but are not limited to the following:

- Correspondence from the requester (which may contain their name, address, phone#, etc.)
  - Incoming request letter
  - Clarification letter
  - Fee agreement letter
- Correspondence to the requester (which may contain their name, address, phone #, etc.)
  - Acknowledgement letter
  - Final response letter
  - Redacted responsive records
- Document management files
  - Original (un-redacted) responsive records
  - Redacted responsive records

1.2 What are the sources of the information in the system?

Individuals who submit FOIA requests to OCC; individuals who appeal OCC denial of their FOIA requests; individuals whose requests, appeals, and/or records have been referred to OCC by other agencies; and, in some instances, attorneys or other persons representing individuals submitting such requests and appeals, individuals who are the subjects of such requests, other government litigators and/or OCC personnel assigned to handle such requests or appeals.

1.3 Why is the information being collected, used, disseminated, or maintained?

FOIAXpress will assist the agencies and Department in tracking, managing and reporting FOIA and Privacy Act (PA) requests. The information related to requester, FOIA requests and delivery requirement are captured within FOIAXpress application because FOIA officer needs to analyze the requested information, screen (perfected) those information; and redact the information as per the FOIA regulation, prior to delivering a response to the FOIA requests initiated by a requester.

These information also may be needed in future in case of an Appeal process is initiated which requires FOIAXpress to maintain the collected information as per the agency's regulation.

1.4 How is the information collected?

The FOIAXpress electronically creates requests, stores requester details, and redacts responsive documents for delivery to requesters. It also tracks FOIA processing statistics/fees and generates reports on the number/types/disposition of requests, as required by the U.S. Department of Justice (DoJ). Additionally, with the implementation of the Public Access Link (PAL), requesters may create and track their submissions online.

1.5 How will the information be checked for accuracy?

OCC employees and contractors processing FOIA requests will enter data into the system and validate the data after entry.

Using the Public Access Link (PAL) the public will have the ability to enter, check, and change their information as needed.

FOIAXpress provides an 'audit report', which details 'what event occurred' (e.g. the action taken), 'when' (e.g. date/time), where the event occurred (e.g. specific feature/function), the source of the event (e.g. user's IP address), and identify (e.g. user).

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

FOIA records are retained in accordance with National Archives and Records Administration's General Records Schedule 14. The General Records Schedule 14 covers certain records pertaining to informational services performed by Government agencies in their day-to-day affairs and in their relations with the public, including records created in administering Freedom of Information Act and Privacy Act (FOIA) programs. These records consist of inquiries, replies, and related correspondence; in the case of FOIA, Privacy Act, and mandatory declassification files, appeals and other records; administrative background files for formal information releases, and records relating to inappropriate release of privileged information.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The exposure is mitigated by safeguarding records in this system in accordance with applicable rules and policies, including all applicable Organizational Common Control systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have been granted system access rights, and those who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

2 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The FOIAXpress data meets the administration's goal for transparency by providing greater visibility into backlogs, and the timeliness of responses, and allowing the requestor, the agencies and the Department to monitor the status and progress of the FOIA request. FOIA officer needs to analyze the requested information, screen (perfected) those information; and redact the information as per the FOIA regulation, prior to delivering a response to the FOIA requests initiated by a requester. These information also may be needed in future in case of an Appeal process is initiated which requires FOIAXpress to maintain the collected information as per the agency's regulation.

2.2 What types of tools are used to analyze data and what type of data may be produced*?*

The system does not analyze the data inside the record. The system's primary function is to track FOIA cases and provide analytical data on the number of open cases, late cases, number of appeals and other statistical data.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

N/A

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses*.*

Only authorized individuals have access to the system. The system is role and privileges based and the application separates publicly available content using different modules not interconnected to the FOIAXpress that resides on the intranet, accessed by OCC personnel via application authentication and PAL that resides on the Internet and accessed by the public in the DMZ (with its own separate web and DB servers).

3 Retention

3.1 How long is information retained?

The retention period of FOIA records in litigation are retained for ten years after the end of the fiscal year in which judgment was made or when all appeals have been exhausted, whichever is later. If the FOIA record deals with significant policy-making issues, it is a permanent record. A permanent record is one that has been determined by the National Archives and Records Administration (NARA) to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period has been approved by the Records Manager and the National Archives and Records Administration (NARA)

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk to the individual is moderate. The primary purpose of FOIAXpress is to track FOIA request with real-time tracking, management, centralized oversight, and quality control across the OCC FOIA program. FOIAXpress will automate the process of capturing, collating, and calculating values for the Annual Report. The OCC FOIA Officer will be able to maintain a real time snapshot of the activities of every agency.

The FOIA information is retained in accordance with a DoJ Freedom of Information Act regulation and as per OCC retention schedule. Privacy risks include improper disclosure of information. These risks are mitigated by limiting access to application and data to individuals that have a valid need-to-know and also limiting the access with Role based access restrictions.

4 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Office of the Comptroller of the Currency.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information in this system will be shared with one or more internal organizations for the purpose of fulfilling the FOIA request. The information will be shared among FOIAXpress users (those that have access to the system, and appropriate privileges) within the OCC FOIA program. The information will be shared with other FOIA Officials in the fulfillment of FOIA or Privacy Act requests.

4.2 How is the information transmitted or disclosed?

With respect to responsive records to requests, the information within FOIAXpress can be printed and/or emailed to the requester. Depending on nature of FOIA requests, information may be disclosed by FOIA office relating to FOIA and Privacy reporting requirements. After proper review and screening, the information may be redacted as needed prior to disclosing and delivering the information content. The FOIA response can be transmitted via email, mail or web download available via Public Web module of FOIAXpress.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

FOIAXpress has the ability to store the requester's information, such as name, address, phone number, email, etc. and FOIAXpress users will have access to their own data via the Public Access Link. The information shared within the confines of the system boundaries. As such, any

individual accessing the information must have appropriate system roles and privileges. System roles and privileges are controlled by the System Administrator. Sharing of information in the system will take place amount Departmental FOIA officers with the appropriate privileges.

FOIAXpress also has auditing features to record which FOIAXpress user accessed the system, when and what they did.

5 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to OCC which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

N/A

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of OCC.

The Department does not intend to share PII data outside the Department. Information shared will be aggregate for the annual report and will be provided to the Department of Justice.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission*?*

Not applicable. The department does not intend to share PII data outside the Department. Information shared will be in aggregate for the annual report.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There are no anticipated risks as PII information will not be shared outside the Department. Only aggregated, statistical, non-PII information will be shared.

6 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The Logon warning banner includes the following text: (The displayed text can be changed or defined thru PAL configuration prior to implementation)

**********WARNING**********

- OCC is authorized to obtain certain information under Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law No. 106-554, codified at 44 U.S.C. 3516, note). Information is needed by OCC to process the request for correction and allow OCC to reply accordingly. This information is needed by OCC to respond to the requestor and initiate follow-up contact with the requestor if required.

- Requestors are advised that they do not have to furnish the information but failure to do so may prevent their request from being processed. The information requestors furnish is almost never used for any purpose other than to process and respond to their request. However, OCC may disclose information to a congressional office in response to an inquiry made on behalf of the requestor, to the Department of Justice, a court, other tribunal when the information is relevant and necessary to litigation, or to a contractor or another Federal agency to help accomplish a function related to this process.

- Requestors should not send OCC their Social Security Number, or other personally identifiable information (PII), such as bank check images, or an image of their state driver's license or an equivalent identification card.

**********WARNING**********

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The only intended use of the information is the FOIA process. Users of the Public Access Link (a web page) system consent to this use upon entering data into the system and submitting a request.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The system requires the users to create a user name and password. User of the system will be given notice that they are using a federal system, and the information collected will be used to process the FOIA. The public can decide not to use the system and submit their FOIA request in hard copy.

7 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

The public user of the system can gain access and update their information in the system under their account user profile.

The public user may submit a Privacy Act request to the Department Privacy officer or the Agency Privacy officer.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If the department has incorrect information on a requester or their respective records, then that data can be updating as needed in the system by the FOIAXpress user/requester.

FOIAXpress user may update their profile in FOIAXpress themselves. If they are unable to resolve the problem in FOIAXpress, the user can contract the AINS FOIAXpress held desk. Contact information will be posted on the FOIAXpress public access link site.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals will receive notification of the procedures for editing their information on the Public Access Link (PAL) from the OCC FOIA website.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Individuals can contact the OCC Privacy Officer or FOIA Officer to address redress problems.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There are limited privacy risks in regards to redress. Redress will be handled primarily in the system.

8 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Only those directly involved in the processing of FOIA requests, the FOIA annual report will have privileges. The System Administrator will assign rights to the FOIA Officers. The FOIA Officers or system administrator for each agency will grant privileges to individuals supporting the FOIA process based on role.

A request for access may be made by OCC management/FOIA Officer to add a user to the system. Upon approval, then the respective FOIAXPRESS system manager will add the user and delegate the appropriate privileges.

8.2 Will Department contractors have access to the system?

Yes.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Users of the system receive annual Information Security Awareness training and Rules of Behavior training. Some personnel may also receive computer security awareness training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

No, The Certification & Accreditation will be complete in September 2012.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Web and Application Server logging provide detailed records of what was accessed, when it was accessed and by whom it was accessed. The FOIAXpress application employs role-based access that provides the minimum level of access needed to perform tasks. The application also provides detailed audit log within the system and the level of auditing can be configured as per agency's need. The audit log is capable in capturing every action that is performed in application by any authenticated user.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Due to the small number of personal data elements collected and the limited sharing of the data the privacy risk is very low. Additionally, because of role and privileges based access the risk of individual of data sharing is very low. Privacy risks include improper disclosure of data by employees. Controls to mitigate this risk include logical access controls and auditing.

9 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

It is mandated system that is in development status.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

10 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Third party websites are not being used. FOIAXpress application is hosted at AINS and accessed with a given .gov application URL by OCC.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Third party websites are not being used. N/A

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Third party websites are not being used. N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Third party websites are not being used. N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Third party websites are not being used. N/A

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Third party websites are not being used. N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Third party websites are not being used. N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or

applications require either the creation or modification of a system of records notice (SORN)?

Third party websites are not being used. N/A

10.10 Does the system use web measurement and customization technology?

Web measurement and customization technology is not being used. N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Web measurement and customization technology is not being used. N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Web measurement and customization technology is not being used. N/A

Responsible Officials

OCC

Approval Signature

_____

Name:

Title:

OCC