U.S. OFFICE OF SPECIAL COUNSEL

PRIVACY IMPACT ASSESSMENT FOR THE FOIAXPRESS SYSTEM

May 2017

Introduction

In September 2013, the U.S. Office of Special Counsel (OSC) entered into a contract with AINS Inc., an information technology (IT) business headquartered in Gaithersburg, Maryland, for an annual subscription to its FOIAXpress (FX) and Public Access Link (PAL) products designed to improve the agency's Freedom of Information Act (FOIA) business processing systems. This Privacy Impact Assessment is prepared in order to address the current state of OSC's use of the FX/PAL products.

1: Types of Personally Identifiable Information (PII) that OSC will collect

Individuals who choose to submit FOIA/PA information requests to OSC through the PAL will submit their PII themselves at the time of registration. Individuals who submit requests to OSC by email, fax, or mail, will submit PII through those methods (in which cases, OSC will enter the necessary PII into FX for the purposes of tracking, processing, and responding. FOIA/PA requesters can submit the PII described below.

A. FOIA/PA requesters submit PII such as names, contact information (address, telephone, email), employing agency or entity, certification of identity.

B. FOIA/PA requesters who seek information about other individuals related to actual or suspected case files sometimes submit third-party PII. Such PII can include descriptions of alleged wrongdoing (if applicable, and which could include the PII noted in item 1, above, about third party individuals), medical information (although most OSC requesters and filers do not provide medical information), and, in limited instances, Social Security Numbers (SSNs). OSC does not require FOIA/PA requesters to submit SSNs. (In some case files related to OSC's administration of matters Under the Uniformed Services Employment and Reemployment Rights Act, the Act required OSC to collect partial SSNs from 2005 to 2007 and 2011 to 2014.)

C. Some FOIA/PA requesters who seek information about deceased third-party individuals will submit relevant proof of death (although most FOIA/PA requests to OSC neither need nor include it).

D. OSC will collect the types of PII noted above when necessary for litigation purposes related to our statutory mission.

2: OSC's reason for collecting or maintaining the PII

OSC selected the FX/PAL products for the management and processing of its FOIA and Privacy Act (PA) requests from the public. FX and PAL provide OSC's FOIA/PA staff with a centralized database to accept secured web-based requests, process requests, track and manage FOIA/PA requests, and produce required statistics and reports for the U.S. Department of Justice.

The FX product is a web-based, commercial, "off the shelf" (COTS) application for processing FOIA and PA requests. Public Access Link allows the public to make their FOIA or PA requests through the web

and track their submissions online. Together, FX and PAL assist OSC's business processes. The FX/PAL software as a service platform, eCase, is FedRAMP certified. The use of such technology enables increased efficiencies and greater services to the FOIA/PA requester community.

3: OSC's intended uses of the PII and how OSC will share it

OSC will use the PII in order to conduct the FOIA/PA functions discussed in this assessment. In order to accomplish those functions, OSC will share the PII within the agency on a need-to-know basis. In addition, OSC previously established Privacy Act routine uses permitting disclosures of some PII outside of the agency. OSC established these routine uses through the notice for the following system of records: OSC/GOVT-1 (OSC Complaint, Litigation, Political Activity, and Disclosure Files). See 77 FR 24242 (Apr. 23, 2012).

Generally, OSC will use the PII in order to process requests, respond to requesters, and fulfill the agency's FOIA/PA obligations. OSC uses PII such as requesters' names and contact information in order to track, process, and respond to requests. For example, we collect a requester's contact information at the start of the request process. We maintain the PII within FX in order to track the status and history of the request and assign relevant tasks. We might add PII to the request file when scanning responsive records for processing, or when creating responsive correspondence.

OSC will not include PII in the reports generated to fulfill FOIA statistical reporting obligations.

4: Methods to decline to provide PII or to consent to particular uses of it

OSC does not require individuals to request information from OSC. An individual who chooses to submit a FOIA/PA request must submit it in accordance with OSC regulations. OSC's regulations permit OSC to request information about a requester's identity. In addition, OSC's regulations require that each requester reasonably describe the records he or she seeks. A requester can decline to provide the necessary PII, and, thereby, stop the FOIA/PA request process at that point.

When processing a FOIA/PA request, OSC may locate records or information that another agency originated. In such instances, OSC's regulations permit OSC to refer to disclose the records or information to the originating agency for response assignment or consultation purposes. When such instances involve an OSC complainant who is the FOIA/PA requester, OSC seeks that requester's consent prior to engaging the other agency. If the requester wants OSC to process such records, he or she would choose to provide the requested consent.

5: How OSC will maintain and secure the PII

OSC will maintain its FOIA/PA records pursuant to the National Archives and Records Administration's General Records Schedule 4.2.

OSC purchased a limited number of FX licenses, and only authorized users will have access to the system. The system requires both a user ID and a password to gain access to the PII. AINS and OSC grant access only to OSC's authorized FOIA staff. To guard against unauthorized access to PII in FX, OSC takes the steps discussed below.

A. All FOIA/PA staff must satisfactorily complete initial and annual IT security awareness training on, and are required to adhere to written OSC policies regarding use of OSC's IT resources and protection of PII and non-public information.

B. Authorized staff users are assigned access protocols and must sign a User Agreement as part OSC's onboarding process, and acknowledge OSC's IT Security sign on banner before logging into their computer system.

C. OSC provides access to FX/PAL on a need-to-know basis using a role-based system. For example, OSC assigns user licenses only to staff with FOIA/PA duties who need to access the system in order to perform those duties. In addition, requesters registered through a PAL account have FX access to the information related to their own account.

D. OSC's risk management team meets quarterly, and as needed, to determine necessary proactive or reactive steps. In addition, OSC's breach response team convenes as needed to identify the scope of potential incidents and take appropriate actions.

E. AINS is a FedRAMP-certified vendor. AINS hosts OSC's FOIA/PA FX data. The data is encrypted at rest and in transit, and AINS generally staff do not have access to the PII. In limited instances, OSC provides administrator access to AINS when necessary to engage system support. Following such instances, OSC changes the administrator password.

F. OSC provides encryption-enabled computers to staff for official use.

6: Privacy Act System of Records

OSC uses the FX product to track and maintain some PII and other information pertaining to FOIA/PA matters pending at any time during FY 2014 and later. The information in this system is contained in the OSC/GOVT-1 Privacy Act systems of records, and OSC is not adding new categories of covered records or individuals.

Approval and Signatures

Date: 5/18/2017

Jennifer Li,
Chief Information Officer

Date: 5/18/2017

Joseph Do,
Chief Information Security Officer

Date: 5/18/2017

Kenneth Hendricks,
Clerk of the U.S. Office of Special Counsel