U.S. OFFICE OF SPECIAL COUNSEL

Privacy Impact Assessment

OSC Enterprise System
(Including the Electronic Case Management System)

January 2017

Introduction

In 2016, the U.S. Office of Special Counsel (OSC) migrated its information technology (IT) services a FedRAMP-approved government cloud hosted by Microsoft. OSC's cloud-based operations will include a new enterprise IT solution. The enterprise solution will include an electronic case management system (eCMS), built on Microsoft Dynamics Customer Relationship Management (CRM) platform. The eCMS will receive, track, and manage allegations and disclosures (and related records) relevant to our statutory jurisdiction, as well as requests for information (and related records). OSC's enterprise IT system includes Microsoft products for creating and managing emails, documents, and OSC case files. OSC selected the vendor Webfortis (name changed to Avtex) in [2015] to develop the enterprise system.

This privacy impact assessment (PIA) is prepared in order to address the current state of OSC's cloud usage and eCMS development stage. OSC will update this PIA once eCMS development is completed.

1. Types of Personally Identifiable Information (PII) that will be collected

A. PII provided by filers of allegations of wrongdoing can include name, contact information (address, telephone, email), employing agency (if applicable), certification of identity, description of the alleged wrongdoing (if applicable, and which could include the above-noted PII about third party individuals); medical information (if applicable, although most OSC filers do not provide medical information). Some case files related to OSC's administration of matters under the Uniformed Services Employment and Reemployment Rights Act required OSC's collection of partial Social Security Numbers, from 2005 to 2007 and 2011 to 2014.

B. PII provided by filers requesting information can include name, contact information (address, telephone, email), employing agency (if applicable), certification of identity, description of requested records (which could include the above-noted PII about third party individuals). Some individuals requesting information about deceased third-party individuals will submit relevant proof of death (although most requests for OSC information neither need nor include it).

C. Some PII regarding OSC employees and applicants resides in the enterprise system. Such PII can include name, Social Security Number, names of family members and beneficiaries, contact information (address, telephone, email), medical information (if applicable).

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

2. **Reason the PII is being collected or maintained**

A. PII is collected from filers of allegations of wrongdoing in order to investigate or review the allegations, arrange necessary follow up activity at OSC or another agency, make conclusions, seek corrective action (if necessary), and track the case files.

B. PII is collected from filers of information requests in order to process and respond to the requests, and in order to track the request files.

C. PII regarding OSC employees is collected or maintained in order to administer necessary human resources functions.

D. Litigation activities require the collection or compilation of PII for litigation purposes.

3. **Intended uses of the PII and how it will be shared**

OSC will use the PII in order to conduct the functions discussed in section 2, above. 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 notices for the following systems of records: OSC/GOVT-1 (OSC Complaint, Litigation, Political Activity, and Disclosure Files); OSC-2 Personnel Security Records); OSC-3 (Pay Management Records).

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

Individuals are not required to file complaints, disclosures, or requests for information. Individuals who choose to file may be required to submit some PII to OSC in order for OSC to conduct necessary activities, or provide the requested responses. Individuals filing complaints and disclosures have the option of declining consent for OSC to discuss the filers' identities with subject individuals and agencies.

OSC is required to collect certain PII for internal OSC human resources purposes. Individuals are not required to seek or retain employment with OSC, but will be required to submit certain PII for application and employment proposes.

5. **How the PII will be secured**

To guard against unauthorized internal access to PII, OSC takes the steps discussed below.

A. All agency staff and contractors are subject to security background checks and successful adjudication as part of OSC's onboarding process for new IT users.

B. All staff and contractors 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.

C. Authorized staff users are assigned access protocols and must sign a User Agreement as part OSC's onboarding process. Office 365 maintains a separate system log as a default security feature.

D. OSC provides access to system functions on a need-to-know basis using a role-based system. For example, a manager's written authorization is required before the Information Technology Branch (ITB) assigns a user to an eCMS role. Under this approach, an employee will receive access only to his or her assigned case information. Employees in a management role will necessarily have access to information from cases assigned to his or her unit.

E. OSC segregates system user roles among business units. Unit managers must grant access to cases for specific work assignments and official duties. For example, investigators from different units will have access to other units' cases only when the relevant units' supervisors grant permissions on need-to-know bases.

F. OSC's risk management team meets [schedule] 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.

G. The enterprise system resides in the FedRAMP-approved Microsoft government cloud. User actions take place through a modern browser, with support for secure hypertext transport protocol (HTTPS) within an encrypted connection. In addition, OSC provides encryption-enabled computers to staff for official use.

H. Privacy Act System of Records

The information in this system is contained in the three OSC Privacy Act systems of records discussed in section 3, above. OSC will publish appropriate systems of records modification notices to reflect usage of the government cloud. The new enterprise system and government cloud usage does not require OSC to modify existing routine uses for these systems of records, and OSC is not adding new categories of covered records or individuals.

I. Information life cycle considerations

The eCMS system will manage and track information form creation or upload, on through permission–based assignments in subsequent stages. In addition, the system provides the capability for automated records management functions. OSC will integrate approved records scheduling provisions into the system to automate retention protections and approved disposition instructions.

Approval and Signatures

_____ Date: _____

Jennifer Li
Chief Information Officer

_____ Date: 1/13/2017

Joseph Do
Chief Information Security Officer

_____ Date: 1/13/2017

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