Privacy Impact Assessment for

Office of Legislative Affairs (OLA)

October 30, 2025

Contact Point

Anthony Ramirez

Senior Advisor

Office of Legislative Affairs (OLA)

Reviewing Official

Becky Ronayne

Senior Agency Official for Privacy

Abstract

This Privacy Impact Assessment (PIA) is being conducted for the Office of Legislative Affairs (OLA) Tracking and Constituent Services Portal (OLA Tracking & CS Portal) system. Each year, OLA receives hundreds of inquiries from congressional staffers on behalf of their congressional office or someone in their district. The system is comprised of two components: OLA Tracking is used to manage the entire lifecycle of the inquiries, and CS Portal is a secure web interface where congressional staffers can submit the inquiries and other messages to the Office of Personnel Management.

This is a replacement to an older system that was decommissioned in November 2023. The new system uses a cloud-version of Microsoft Dynamics 365, Dynamics Portal, Dataverse, and SharePoint Online. The system collects personally identifiable information as part of regular OLA business processes.

Overview

OPM Office of Legislative Affairs (OLA) Constituent Services (CS) handles inquiries from congressional staffers (staffers) asked on behalf of their congressperson or constituents. These constituents are often annuitants, survivor annuitants, or current or former federal employees. The inquiries are often about retirement, health care, or other OPM programs and policies. OLA CS uses the OLA Tracking & CS Portal system to log the inquiries from staffers, route the inquiries to the appropriate OPM program offices for action, track when and how OPM responded to the staffers, and create reports about that work.

CS Portal is a secure web interface that staffers can use to submit inquiries and associated documents, track the status of that inquiry, and send messages and documents about that inquiry to OLA CS staff. No data or files are retained or stored in the CS Portal.

To access the CS Portal, staffers must register and create an account, which requires them to verify their identity through multifactor authentication. Each staffer account request is reviewed and approved by OLA CS staff.

OLA Tracking creates a new case file for each inquiry. It tracks the receipt and processing of the inquiry, records connected to the inquiry, relevant deadlines, and other key events or data (including OPM's response to the inquiry and any records gathered to help respond). OLA Tracking also links together all the inquiries submitted by or on behalf of the same constituent.

For each inquiry, the OLA Tracker maintains contact information for the staffer, their congressperson, and the OLA CS representative. If an inquiry is about a constituent's personal record, the staffer must provide the constituent's full name, a copy of the constituent's privacy release authorization, and details about the inquiry. That may include additional personally identifiable information (PII) such as the constituent's contact information, Social Security Number (SSN), annuitant claim numbers, compensation claim numbers, insurance account numbers, insurance claim numbers, military serial numbers, birth date, financial institution routing number, and financial institution account number.

OLA Tracking also stores all communications and documents connected to the inquiry. This may include letters, emails, and attachments between OPM and the staffer, constitution, or other parties that may have information to help answer the inquiry (e.g., other federal agencies). This may also include legal, administrative, or similar non-public agency records relevant to the inquiry. These communications and documents can include additional PII about the respondent, constituent, and others.

The new system uses a cloud-version of Microsoft Dynamics 365, Dynamics Portal, Dataverse, and SharePoint Online.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

5 U.S.C. 301 and 44 U.S.C. 3101 enable OPM to establish systems and procedures to collect information and allow OLA to manage and maintain records to provide services to congresspeople, congressional staff, and constituents. We rely on the authorities in EO 9397, as amended by EO 13478, to accept the SSN of the person requesting services from their congressperson regarding an issue with OPM.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The records in this system are covered OPM/INTERNAL-21, Correspondence Management for the U.S. Office of Personnel Management.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes. A System Security Plan for Application Development Tools (ADT) was completed on March 26, 2024, in connection with the ADT Authority to Operate (ATO).

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

OLA is currently working with the OPM Records Management Office to finalize the records retention schedule.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

For all inquiries, the OLA Tracker maintains contact information for the staffer, their congressperson, and OLA CS representative. For inquiries about constituents' personal records, the OLA Tracker may collect PII including constituent names, addresses, phone numbers, email addresses, SSNs, annuity claim numbers, compensation claim numbers, insurance account numbers, insurance claim numbers, military serial numbers, birth dates, financial institution routing numbers, and financial institution account numbers. PII about additional individuals may also be included in records used to respond to the inquiry.

2.2. What are the sources of the information and how is the information collected for the project?

Information may be collected from members of the public, private sector entities, OPM employees/contractors, employees/contractors of other federal agencies, congressional staffers, congresspeople, and OLA CS representatives. That information may have originally been collected from the subject via verbal, paper, and electronic collections.

The information often comes in response to a request from a constituent. When that occurs, OLA Tracker needs enough information to enable OPM to identify the records they already have on the constituent and verify their identity.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4. Discuss how accuracy of the data is ensured.

For data provided by congressional offices, OLA validates that data against information in OPM internal records and by corresponding directly with the

congressional staffer and/or the constituent. For data provided by internal offices, OLA validates that data by corresponding directly with the program office and by conducting additional internal checks, as appropriate.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more PII than is necessary for the resolution of the congressional inquiry will be collected and maintained in the system.

Mitigation: This risk is mitigated through the establishment of procedures to avoid unnecessary collection of PII and to remove unnecessary PII if it is collected inadvertently. In addition, PII that is stored and transmitted through the system is done through secure connections and encryption of PII so that exposure is limited.

Privacy Risk: There is a risk that the information collected or stored in the system is not accurate.

Mitigation: This risk is mitigated through the establishment of procedures to verify the accuracy of data, to include verifying the accuracy of data provided by congressional offices and verifying the accuracy of data collected by internal program offices.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The application is used to track and report on correspondence for the OLA program office. The application manages various correspondence types through a defined workflow, routing items to other OPM program offices for input/action, as required.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

No.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

OLA Tracking allows OLA CS staff to refer an inquiry to another OPM office so they can review the inquiry and provide a response. The following OPM program offices have access to the system: Workforce Policy and Innovation (WPI), Human Capital Data Management and Modernization (HCDMM), Healthcare and Insurance (HI), Human Resource Solutions (HRS), Merit Systems, Accountability, and Compliance (MSAC), Office of the Chief Financial Officer (OCFO), Office of the Director (OD), Retirement Services (RS), Facilities, Security and Emergency Management (FSEM), OPM Human Resources, and Suitability Executive Agent (SUITEA).

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The privacy risk includes the inadvertent/unintentional disclosure of PII to sources that do not need that information. There is a risk that an authorized user may access information for an unauthorized purpose or that an unauthorized person may gain access to the system.

Mitigation: The risk is mitigated by requiring staffers to log in using a unique identifier, a password, and multifactor authentication. Risk is also mitigated by limiting the individuals with access to the system and by limiting what each user can access within the system. For example, staffers are limited to viewing only cases for constituents of the congressperson' district. In addition, OLA CS will release information only to staffers who are registered in the system or otherwise verified by OLA CS staff.

Section 4.0. Mitigation: Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

OPM only acquires PII from staffers who choose to submit an inquiry to OPM. When that inquiry involves a constituent, the constituent has given prior consent in writing and approval to the staffer to 1) access their information and 2) provide enough information to OPM to allow OPM to identify and access the correct records for a response. Notice is also provided indirectly through the publication of the relevant System of Records Notices.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Congressional inquiries are an opt-in information collection activity. Without the prior consent of the individual, OPM cannot provide information to the constituent or the congressional office. Therefore, individuals can decline to provide all the information, however, this may impede or preclude the individuals from receiving a response to their inquiry.

OPM does not provide PII to constituents or congressional offices without privacy release forms being provided.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: The individual may not be aware that the collection of information by the congressperson's office is taking place for the purpose of sending it to OPM.

Mitigation: The risk is mitigated through the congressperson's office obtaining the individual's signature on the Privacy Release form which contains a Privacy Act Statement. These risks are also mitigated by OPM posting Systems of Records Notices and OPM Policies regarding the collection of information.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Information about an individual is maintained in the system to keep a record of the interaction with the congressperson and to enable better customer service should the individual contact the congressperson or any other congressperson about their issue(s) in the future. Information may also be retained indefinitely for historical research purposes.

OLA is currently working with the OPM Records Management Office to finalize the records retention schedule.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: This privacy risk includes the retention of PII which is no longer needed for processing or PII that is past its retention date.

Mitigation: These risks are mitigated through a variety of system security controls to include the establishment of a retention policy, establishment, and use of a SORN, and automated retention processes.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OLA CS staff share information about specific cases (including relevant PII) with other agencies and elsewhere as needed to complete requests from congressional offices and/or constituents. PII is only shared if OPM has a privacy release on file for the case.

Information enters the OLA system via staffers. The responsive information from OPM will be shared with the Legislative Branch as per normal agency operations. Each Congressperson's office uses their own privacy release form; our understanding is that the forms are used in accordance with the Privacy Act. In general, the privacy release forms affirm that any information or records of the individual may be released to the office to aid in resolving the issue, including, but not limited to information and records covered by privacy laws.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The information sharing described above is in accordance with OPM/INTERNAL-21. This includes routine use (c): *For Congressional Inquiry—To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.*

6.3. Does the project place limitations on re-dissemination?

No. There are no express limitations on re-dissemination of the information obtained from the Congressperson's office that we are aware of. Because, as we understand it, the Congressperson's office may share as necessary to respond to the constituent. OLA does not share with anyone outside of OPM beyond the routine uses mentioned in 6.2.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

OLA tracking maintains records of all communications to staffers, including when OLA CS provide a final response addressing/closing the congressional inquiry.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The potential risk associated with external information sharing includes unauthorized access to PII.

Mitigation: When OPM becomes aware that staffers inadvertently received paper or electronic PII that is not related to their constituent, we report to

the OPM cybersecurity team and ask the relevant receiving office to shred or destroy the documentation in their systems.

Privacy Risk: This privacy risk includes the inadvertent/unintentional disclosure of PII to sources that do not need to have that information through information sharing.

Mitigation: When OPM becomes aware that an individual or office inadvertently received paper or electronic PII that is not related to the constituent, we report to the OPM cybersecurity team and ask the relevant individual or office to shred or destroy the documentation in their systems.

Section 7.0. Redress

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

This system is for the collection and transmission of information between OPM and the Legislative Branch. Staffers who want access to their information could request it from OPM via the CS Portal or by directly contacting OLA. Constituents could also contact OLA directly, but since they generally interface with their congressperson instead of OPM, they would be far more likely to contact that congressperson for access to their information. Depending on the type of records requested, individuals may be asked to furnish their full name, date of birth, SSN, last employing agency (including duty station and approximate date(s) of employment (for former federal employees), and signature.

All individuals may also request access to their Privacy Act covered information in OLA Tracking by following the procedures set out in the OPM/INTERNAL-21 SORN. Individuals must furnish certain information for their records to be located and identified, including name, date of birth, and SSN. In addition, individuals requesting access must also follow OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

This system is for the collection and transmission of information between OPM and the Legislative Branch. Staffers who want to correct inaccurate information could contact OPM via the CS Portal or by directly contacting OLA. Constituents could also contact OLA directly, but since they generally interface with their congressperson instead of OPM, they would be far more likely to contact that congressperson. Depending on the type of correction, individuals may be asked to furnish their full name, date of birth, SSN, last employing agency (including duty station and approximate date(s) of employment (for former federal employees), and signature.

All individuals may also request access to their Privacy Act covered information in OLA Tracking by following the procedures set out in the OPM/INTERNAL-21 SORN. Individuals must furnish certain information for their records to be located and identified, including name, date of birth, and SSN. In addition, individuals requesting access must also follow OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

7.3. How does the project notify individuals about the procedures for correcting their information?

If a constituent only interfaces with their congressperson, OPM does not have opportunity to directly inform them how they could correct their information, but if the constituent asks the congressperson to help them correct their records, OPM will work with the constituent and congressperson to accomplish that.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to access information about them that is contained in this system or be afforded an adequate opportunity to correct that information.

Mitigation: The risk is mitigated by the ability of the individual to request assistance from the Congressperson or OPM in correcting the information

contained in the system. OLA CS will work with the congressional office and constituent to identify and correct erroneous information, as appropriate.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Only the necessary (minimal) PII needed for the storage, identification and processing of data was included in the system. Subsequent PII noted as not necessary for processing was not included in the new system. The stated practices in the PIA are consistent with OLA business practices, which ensures that information is only used for appropriate business purposes and shared only with appropriate audiences.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees and supporting contractors must complete OPM's annual IT Security and Privacy Awareness Training. Depending on their role, additional training may be provided. We understand that staffers follow the privacy training applicable to the Legislative Branch.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Role-based access controls consist of both administrative processes and management of technical functions that establish who can perform an action, when they can perform it, and how the action can be accomplished. Administrative controls identify users by groups (roles) and associated permissions (e.g., read, write execute, delete, etc.). Roles and permissions are directly associated with the specific job responsibilities that the user performs in accomplishing mission objectives. Technical controls implement the administrative decision by enabling specific group/roles and linking the group/role to allowed permissions within specified system resources. Access security policy is documented in the OPM IT Security Policy and is posted on the OPM intranet.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The business owner must provide the system owner with a fully executed MOU prior to creating a connection to share information from the system.

Responsible Officials

Anthony Ramirez
Senior Advisor
Office of Legislative Affairs

Approval Signatures

Becky Ronayne
Senior Agency Official for Privacy