Office of Justice Programs

Privacy Impact Assessment
for the
OJP Service Portal (OSP)

Issued by:

Maureen Henneberg
Senior Component Official for Privacy

Approved by: Andrew J. McFarland
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: July 9, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

OJP Service Portal (OSP) is a customized version of the ServiceNow Software as a Service (SaaS) platform which is implemented by OJP to efficiently manage, track, and improve productivity of IT operations and to manage and streamline Human Resources (HR) operations. There are two categories of users of OSP: The Internal OJP IT Administrative Users and the End Users, which consist of the Internal OJP Users (OJP Federated Users) and the External Users (Non-OJP Federated Users).

OJP has prepared a Privacy Impact Assessment for OSP because this system collects, maintains, and disseminates Personally Identifiable Information (PII) and Protected Health Information (PHI) of Internal OJP Users. Information collected from Internal OJP users includes DOJ e-mail addresses, office locations, telephone numbers, OJP Automated Data Processing (ADP) and desktop equipment information (either provided by the user or through a discovery tool), and a description of the user's IT issue. The authoritative source for both contacts and internal users is DIAMD. External users will be required to provide their name, email address, telephone number, and a description of the issue. PHI may be collected through this system when OJP employees request family and medical leave, telework, and reasonable accommodations. When PHI is collected, such information may include diagnosis details, doctor's visits, prescription medication details, laboratory test results, medical insurance information, Medicare options, Medicare beneficiary identifiers, and physical handicap codes.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

A. IT Operations Uses of OSP

OSP Information Technology Service Management (ITSM) is used by OJP for change management activities, such as adjusting server configurations, upgrading systems, and deploying new development features to production systems. OSP has a built-in reports development environment, that delivers standardized or customizable reports on process activities to measure performance and identify improvements. OSP provides Knowledge Base articles that provide solutions to common IT issues. OSP will also allow OJP to better manage and track service requests, network outages, and IT access issues across the agency that are reported to the OJP IT Service Desk.

OSP will be operated by internal DOJ/OJP personnel. This includes OJP IT Service Desk personnel and contractors as well as OJP IT professionals working to resolve any

reported issues. OSP access is managed by roles and associated privileges. These include Internal OJP IT Administrative Users and End Users. As explained in Section 1, End Users include Internal OJP Users (OJP Federated Users) and External Users (Non-OJP Federated Users).

- Internal OJP IT Administrative Users: Use OSP for intake, tracking, and resolution of reported IT related issues. This includes reporting and tracking data incidents and breaches involving OJP. These users have privileged roles on OSP and perform system administrator functions for OSP at the ServiceNow platform level and manage system configuration, users, groups, and associated administrative features within OSP.

- End Users: Use OSP to (1) report a case through a ticket to request a service advertised as a customer service and (2) search for knowledge articles (*i.e*. articles that provide solutions to common IT issues) that OJP has categorized as customer accessible (*i.e*., publicly available). End Users have three methods for contacting the OJP IT Service Desk to report an IT-related issue: (1) use the OSP User Portal; (2) email; or (3) phone. For contacts by email or phone, the OJP IT Service Desk personnel enter the user's contact information and reported issue into OSP for tracking purposes. The internal OJP users' contact information comes from the Digital Identity and Access Management Directory (DIAMD). Any additional updates to the user's contact information are made by Service Desk agents when interacting with the customers. OSP business roles are mapped to business functions for the external environment for the specific user type. End Users are further distinguished by whether they are known to OJP at the time of their contact in OSP:
    - Internal OJP Users (OJP Federated Users): These users are mapped to business roles within the business functions. These roles are provisioned as non-privileged roles that can create cases, view and edit cases, and work with customers and subject matter experts (SMEs) to resolve cases.
    - External Users (Non-OJP Federated Users): These users include DOJ Component Users and members of the public who use OJP services, such as JustGrants users. External users must provide their name and contact information (business or personal) so that OJP IT Service Desk personnel can follow-up in response to any reported issues. External users are only able to submit an email to OSP which generates a case record or call the helpdesk and leave a voicemail which will generate a case for the helpdesk.

B. HR Operations Uses of OSP

OJP People Platform (OPP) in OSP is the segregated HR management platform for OJP. It is a comprehensive module designed to streamline and manage HR processes, from onboarding new employees to maintaining accurate employee records and handling various requests. OPP also manages employee requests for updates, benefits, and leave, providing a centralized and efficient platform for these activities. With OPP implementation, external users will be able to access an external facing OPP Employee Portal.

During onboarding of new personnel, necessary information like Social Security numbers (SSNs) and dates of birth are collected for background checks, with sensitive data being securely hashed and encrypted to protect privacy.

C. Other Uses of OSP

The National Criminal Justice Reference Service (NCJRS) database uses OSP to allow members of the public to order publications. If a customer wants to order a publication in the library, they are provided a link to OSP and they will obtain an open ticket by providing a name, address, email, and phone number for their order. The OJP Library Services Team then provides an electronic version of the requested document. If a customer requests a hard copy due to accessibility needs, the OJP Library Services Team will mail a hard copy to them through the open OSP ticket.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	34 U.S.C. § 10102; 28 U.S.C. § 530C
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	First and Last Name
Date of birth or age	X	A & B	The date of birth serves as a static value to correlate with the data from NFC for hashing SSNs in OSP
Place of birth			
Sex	X	A & B	Gender information is collected as a part of the OPP
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A & B	SSN will be protected through hashing within OSP
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A & B	Street number, city, state, and zip code
Personal e-mail address	X	A, B, C, and D	If business contact information cannot be provided (e.g. new hire), personal contact information may be collected
Personal phone number	X	A, B, C, and D	If business contact information cannot be provided (e.g. new hire), personal contact information may be collected
Medical records number	X	A & B	Policy number
Medical notes or other medical or health information	X	A, B, C, and D	Diagnosis details, doctor's visits, prescription medication details, laboratory test results, Medicare options, Medicare beneficiary identifier, accept enrollment (yes/no), has other insurance, other insurance type, other insurance name, policy number, plan, physical handicap code. In the future, HR envisions staff could provide PHI for Family Leave Medical Act (FMLA), Telework Tracker, and Reasonable Accommodations (Form 100A) through OSP

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Financial account information	X	A & B	Locality pay area, locality pay code
Applicant information	X	A & B	Life insurance: plan option, enrollment options a/b/c, effective begin date, effective end date, candidate primary telework street, primary telework city, primary telework state, primary telework zip, has second location, secondary telework street, secondary telework city, secondary telework state, secondary telework zip, gender, live profile
Education records	X	A & B	Education level
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	System admin data
- **User ID**	X	A	System admin data
- **User passwords/codes**	X	A	System admin data
- **IP address**	X	A	System admin data
- **Date/time of access**	X	A	System admin data
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	PII and PHI is only available to staff with a need-to-know and is secured by access controls. Privileged users have the ability to export data for external analysis and reporting. Data exports are monitored and tracked by user ID.
DOJ Components	X			OJP reports all incidents and breaches to JSOC.
Federal entities				
State, local, tribal gov't entities				
Public				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 ***If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.***

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 ***What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.***

Generalized notice is provided by DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records; OPM/GOVT-1, General Personnel Records; and OJP-011, Registered Users File - National Criminal Justice Reference Service (NCJRS). Additionally, OJP provides tailored Privacy Act 552a(e)(3) notices for both internal and external users.

5.2 ***What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

The system does not allow for anonymous access. User account information may be shared with individuals in each office on a need-to-know basis. For internal users the information is collected by Active Directory and users are provided a statement clarifying

that there will be no expectation of privacy as to the use of Federal government equipment (see Notice at 6.2); when each internal user joins the Department, their information will be collected by their consent. Internal users may consent to the collection, uses or dissemination during self-service registration, although they often are required to provide certain information to be able to use the system to perform their job duties. Usage of the system is voluntary for external users, however their usage is subject to their consent to the collection of their information. OJP provides tailored Privacy Act 552a(e)(3) notices for both internal and external users.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

As provided in the DOJ SORN that covers the OJP Service Portal system, individuals seeking to contest or amend records must directly contact the Justice Management Division's (JMD) Freedom of Information Act (FOIA) office. Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "Record Access Procedures" paragraph in the SORN. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request". All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** ATO granted March 2, 2023; expires March 3, 2026. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** N/A

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** The justification of the categorization seems to derive from assessments of Moderate for the Integrity of the system's Information Security, Lifecycle/Change Management, and System Maintenance, as well as the system's adherence to SC-28 which, in inheritance from the DOJ Common Controls Program, requires encryption at rest and during transmission for a minimum of Moderate and High information systems.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** OSP provides user logging that can be imported into OJP Splunk for monitoring. As individual and service accounts are managed by DIAMD, that system provides further monitoring capability.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Auditing is conducted on an annual basis as part of the internal Core Control program.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

OSP adheres either directly or through inherited hybrid controls the suite of Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), Risk Assessment (RA), System and Communications Protection (SC), and System and Information Integrity (SI).

Of these, the only controls confirmed to be implemented are as follows:

- AC-03(07): Role-Based Access Control

- AC-06: Least Privilege
- AC-11(1): Pattern-hiding Displays
- AC-17: Remote Access
- AC-17(2): Protection of Confidentiality and Integrity Using Encryption
- IA-02: Identification and Authentication (organizational Users)
- IA-02(1): Multi-factor Authentication to Privileged Accounts
- IA-02(2): Multi-factor Authentication to Non-privileged Accounts
- IA-06: Authentication Feedback
- IA-07: Cryptographic Module Authentication
- IA-08: Identification and Authentication (non-organizational Users)
- RA-05(2): Update Vulnerabilities to be Scanned
- SC-02: Separation of System and User Functionality
- SC-07(3): Access Points
- SC-08: Transmission Confidentiality and Integrity
- SC-18: Mobile Code
- SC-23: Session Authenticity
- SC-28: Protection of Information at Rest
- SC-39: Process Isolation
- SI-02: Flaw Remediation
- SI-04(2): Automated Tools and Mechanisms for Real-time Analysis
- SI-07: Software, Firmware, and Information Integrity
- SC-12: Cryptographic Key Establishment and Management

Regular auditing of these controls in question as part of OJP's internal Core Control audit program can be used to detect unauthorized access by reviewing the mechanisms employed to grant access and compare them with logs indicating unauthorized access. As OSP is integrated with the Secure Cloud Network (SCN) cloud instance, any logging indicating unauthorized access would be within the purview of SCN, and must comply with OJP SOP 063: Security Audit Logging, Monitoring, and Reporting. Some audit controls for OSP are hybrid implemented with the DOJ Common Controls Program, where not solely applicable, and must be compliant with DOJ Order 0904 and the DOJ Cybersecurity Standard.

Instead of storing SSNs directly, OSP creates a secure, hashed version using a unique code called a salt (a cryptographically secure random string). This hashing process helps match employee records provided by the National Finance Center (NFC), which includes SSNs and dates of birth. When new data comes in, the system generates a hash from the SSN and date of birth, and matches it with existing records. During onboarding, SSNs are temporarily stored in an encrypted format for background checks and then deleted. Only authorized personnel can access or modify this data. If there are mistakes, like an incorrect date of birth, the system requires corrections in both OSP and NFC to ensure accuracy.

6.3 Indicate how long the information will be retained to accomplish the intended purpose,

and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

The records retention schedule covering records hosted on OSP is in compliance with and follows DOJ OJP general records retention polices. Until a records retention schedule is approved by the national Archives and Records Administration, records related to the OSP system will be retained for the purpose of information request verification of user systems issues. Thereafter, the records will be destroyed in accordance with the policy, once the record retention schedule is complete.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

This system is covered by:

- DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf;
- OPM/GOVT-1, General Personnel Records, last published in full at 77 Fed. Reg. 79694 (Dec. 11, 2012), available at: https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/pdf/2012-29777.pdf; and
- OJP-011, Registered Users File - National Criminal Justice Reference Service (NCJRS), last published in full at 58 Fed. Reg. 51879 (Oct. 5, 1993), available at: https://www.justice.gov/opcl/docs/58fr51879.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how

are those risks being mitigated?

OSP contains both PII and PHI information. The scope of OSP data covers operational functions: Infrastructure Change Management, Business Document, and Information Request tracker applications, and lastly operational business stakeholder and grantee inquires covering all OJP platforms. By policy OJP support desks include PII and PHI data in service support tickets, OJP grant account data is limited.

There is a privacy risk to the information arising from potential unauthorized access. OSP mitigates this risk by implementing various security controls such as: role-based access based on need-to-know information, multi-factor authentication for users, and protection of information at rest and during transmission. OSP has the capability to encrypt any data attribute or file identified as sensitive. For example, SSNs and dates of birth are encrypted by hashing. The OSP team sends a clone of production data to the lower development and test environments on a routine monthly basis. Any data attributes deemed sensitive are scrubbed from the cloned data file via data script.

There is also a privacy risk arising from unauthorized dissemination of information. For example, privileged users have the ability to export data for external analysis and reporting. However, this risk is mitigated by monitoring and tracking the data exports by user ID. OSP also does not have any outbound data feeds.