U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Joint Administrative Operations (JAO) Service Center's Case Management System, or "MySupport"
Bureau/Office: U.S. Fish and Wildlife Service
Date: December 10, 2020
Point of Contact:
Name: Jennifer L. Schmidt
Title: FWS Privacy Officer
Email: FWS_Privacy@fws.gov
Phone: (703) 358-2291
Address: 5275 Leesburg Pike, MS: IRTM Falls Church, VA 22041-3803

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The JAO Service Center's Case Management System, also known as "MySupport," is a workload management tool for all U.S. Fish and Wildlife's (FWS) administrative support services. It streamlines workflows via a shared service delivery model for all JAO responsibilities and processes including acquisitions, property and travel management, finance, human resources and safety operations, and facilitates centralized tracking by JAO of all administrative actions and requests from across FWS.

MySupport replaces JAO's previous process of email intake for all requests and inquiries. Instead of sending emails to a general mailbox, employees will use MySupport's intranet portal to submit and track their own requests. This allows for more secure transmission of data, enables faster processing and helps improve JAO's responsiveness to its customers, the personnel of FWS.

MySupport is not an official repository of records. Information is collected and maintained temporarily in MySupport before being manually transferred to the appropriate FWS or enterprise-wide system, as necessary. For example, a JAO specialist will receive a request for a pay adjustment via MySupport. Then, after verifying the information is correct, the specialist will update or correct the employee's information in DOI's Federal Personnel Payment System (FPPS).

MySupport may also be used to measure the JAO Service Center's performance. JAO expects to integrate MySupport with DOI's enterprise onboarding and financial management systems eventually. FWS will update this PIA beforehand to reflect system interconnections and any new or modified sharing of PII.

C. What is the legal authority?

- 5 U.S.C. 1302, 2951, 3109, 3301, 3302, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 3372, 4103, 4118, 4723, 5532, 5533, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
- 5 U.S.C. 5101, et seq., Government Organization and Employees; 31 U.S.C. 3512, et seq., Executive Agency Accounting and Other Financial Management Reports and Plans; 31 U.S.C. 1101, et seq., the Budget and Fiscal, Budget, and Program Information; 5 CFR part 293, subpart B, Personnel Records Subject to the Privacy Act; 5 CFR part 297, Privacy Procedures for Personnel Records; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers; and Public Law 101-576 (Nov. 15, 1990), the Chief Financial Officers (CFO) Act of 1990.
- 5 U.S.C. 5707 and as implemented by the Federal Travel Regulation, 31 U.S.C. 3511, 3512, and 3523; E.O. 12931; 40 U.S.C. Sec. 501-502; 41 CFR 300-304; E.O. 9397, as amended; E.O. 11609, as amended; Public Law 107-56 Sec. 326; Public Law 109-115 Sec. 846; Laws administered by the Department of Treasury, under the Office of Foreign Assets Control (OFAC) Regulations for the Financial Community, dated Jan. 24, 2012 (50 U.S.C. App. Sec. Sec. Sec. Sec. 1-44, 18 U.S.C. 3571, 50 U.S.C. 1701-06, 18 U.S.C. 3571, Public Law 101-513, 104 Stat. 2047-55, 22 U.S.C. 287c, 22 U.S.C. 2349 aa-9, 22 U.S.C. 6001-10, 22, U.S.C. 6021-91, 8 U.S.C., 219, 18 U.S.C. 2332d and 18 U.S.C. 2339b, Public Law 106-120,tit. VIII, 113 Stat 1606, 1626-1636 (1999) (to be codified at 21 U.S.C. 1901-1908, 18 U.S.C. 1001).

- 5 U.S.C. 301, 3101, 5105-5115, 5501-5516, 5701-5709; 31 U.S.C. 66a, 240-243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C. 3101; Executive Order 11807.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☒ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

000000432 Joint Administrative Operations (JAO) Service Center SSP

☐ No:

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None.			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

Due to the nature of MySupport as a case management system for all of FWS’ administrative actions, records may be covered by a Government-wide, Department-wide, or a FWS Privacy Act system of records which may be viewed at https://www.doi.gov/privacy/sorn. The primary SORNs that MySupport relies on are:

INTERIOR/DOI-47, HSPD12 Logical Security Files (Enterprise Access Control Service/EACS) 72 FR 11040 (March 12, 2007)

INTERIOR/DOI-58, Employee Administrative Records, 64 FR 19384 (April 20, 1999); modification published 73 FR 8342 (February 13, 2008)
INTERIOR/DOI-85, Payroll, Attendance, Retirement, and Leave Records 83 FR 34156 (July 19, 2018)
INTERIOR/DOI-88, Travel Management: FBMS, 73 FR 43769 (July 28, 2008)
OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015)
OPM/GOVT-5, Recruiting, Examining, and Placement Records, 79 FR 16834 (March 26, 2014); modification published 80 FR 74815 (November 30, 2015)
GSA/GOVT-3, Travel Charge Card Program, 78 FR 20108 (April 3, 2013)
GSA/GOVT-4, Contracted Travel Services Program, 74 FR 26700 (June 3, 2009); modification published 74 FR 28048 (June 12, 2009)

□ No

H. Does this information system or electronic collection require an OMB Control Number?

□ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Child or Dependent Information
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Other Names Used
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Credit Card Number
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: work email address; occupational series; entrance/separation dates; case number.

The only direct collection of full SSN is limited to new credit card applications for travel and/or purchase cards. Due to the nature of MySupport as a case management system for FWS' administrative services including hiring actions, it may contain sensitive information as listed above to onboard individuals as employees, or amend current employees' personnel records.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Web site (Intranet)
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems *Describe*
☐ Other: *Describe*

D. What is the intended use of the PII collected?

PII collected and maintained in MySupport is used by JAO to receive, track, organize and manage requests for human resource, payroll and other administrative actions for current and prospective FWS employees. For example, supervisors use MySupport to approve and submit employee government purchase and travel credit card applications. Supervisors also request hiring actions through MySupport and may attach sensitive information such as the prospective employee's resume or completed Standard Forms (SF) for employment. Other processes handled through MySupport include but are not limited to: transfers of property ownership; delegations of authority such as Chief Procurement or Collection Officers, and exit clearances.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII from MySupport is not routinely shared with FWS personnel or units outside of JAO. However, it is permissible to share PII with FWS employees and contractors who have need-to-know in the performance of their official duties.

☒Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

PII is manually uploaded by JAO specialists to DOI information technology systems as necessary for the purpose of resolving the individual’s administrative action request. For example, information related to an individual’s pay or leave is shared with DOI’s Federal Personnel and Payroll System (FPPS). Information related to acquisitions, fleet management, or property is shared with DOI’s Federal Business Management System (FBMS). For a description of these DOI systems, their privacy risks and DOI’s mitigations, please see the respective Department-wide PIAs at https://www.doi.gov/privacy/pia#DW.

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☐ Contractor: *Describe the contractor and how the data will be used.*

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

PII is from MySupport is shared with FWS’ credit card vendor in order for employees and contractors to apply for and be issued a government purchase and/or travel card.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

While FWS employees and contractors may not decline to provide PII in order to submit or process administrative action requests, all individuals including prospective employees, receive notice of how their PII may be used and shared for employment purposes during the hiring and onboarding process.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

MySupport provides a Privacy Act Statement to users on the login page. Privacy Act statements are included also on Standard Forms (SF) used during the hiring and onboarding process.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and related SORNS published in the *Federal Register*. Please see the SORNs on the DOI SORN website at https://www.doi.gov/privacy/sorn. More information about the Department’s privacy program including compliance documents and how to submit a request for agency records protected by the Privacy Act of 1974 is available at DOI’s Privacy website at https://www.doi.gov/privacy.

☒ Other: *Describe each applicable format.*

Users are provided with a DOI security warning banner upon network logon that they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved by case number and/or record subject’s full name.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*

☒ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data maintained in MySupport is generally obtained directly from the record subject and therefore presumed to be accurate. It is the responsibility of the requesting employee to ensure his or her request is accurate. Employees may contact JAO at any time to modify or cancel their requests. JAO employees responsible for the intake of requests help to ensure accuracy also by checking the request for any errors before submitting to a JAO specialist for action and/or sharing with DOI.

B. How will data be checked for completeness?

Data maintained in MySupport is generally obtained directly from the record subject and therefore presumed to be complete. It is the responsibility of the requesting employee to ensure his or her request is complete. Employees may contact JAO at any time to modify their requests. JAO employees help to ensure completeness by checking the request for any missing information needed in order to complete the request. Incomplete requests are returned to the submitter.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data maintained in MySupport is generally obtained directly from the record subject and therefore presumed to be current. It is the responsibility of the requesting employee to ensure his or her request is current. Employees may contact JAO at any time to modify their requests. JAO specialists help to ensure that the data is current by verifying the employee's request and making sure that the requested action is needed before sharing with any DOI system. Requests that are found to be inaccurate, incomplete or not current by JAO's multiple layers of review are returned to the requesting employee.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records in MySupport are considered temporary and are destroyed after three years in accordance with Department Records Schedule 1 – Administrative DAA-0048-213-0001 for Short Term Administrative records, approved by the National Archives and Records Administration (NARA).

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to individual privacy due to the PII collected and maintained in MySupport. The primary risks to privacy are unauthorized access and/or misuse of the data, and collecting more information than necessary. There are also privacy risks posed from lack of system notice, the possibility of retaining information longer than necessary and inaccurate data caused by manual entry to DOI systems.

These risks are mitigated. Unauthorized system access and misuse of the data are mitigated by authenticating all users and controlling access. MySupport implements role-based access control using the principles of least privilege and limiting access to the MySupport backend on a need-to-know basis. Standard users are not granted access to employees PII and can only view MySupport data at the aggregate level. JAO employees also receive specific training for their role and how to best keep employees’ PII secure. For example, JAO specialists responsible for the manual entry of MySupport data into DOI systems are training and acknowledge the importance of double-checking their transcription to catch any errors.

The risk of collecting more information than necessary is mitigated by MySupport’s quality assurance process and multiple layers of review. Part of this process includes deleting or returning to the individual any documents or information that is irrelevant or unnecessary. For example, if a requester submits a picture of prospective employee as part of the supporting documentation, the JAO specialist responsible for intake of the request would delete the photograph. MySupport’s automated records disposition mitigates the risk that records or information may be stored longer than necessary. Records older than 3 years and no longer needed for any business purpose are purged from the system JAO specialists are trained to delete records that are unnecessary or redundant and verify all request information before sharing with the appropriate office or system for action. Cases will be regularly spot-checked in accordance with JAO MySupport User guidelines.

There is also some privacy risk associated with lack of notice for the system. Users do not have the opportunity to decline to provide their information in order to access the system, or the option to not use the system when they need to submit or process an administrative action request. This risk is mitigated by notices provided during the hiring and onboarding process. These notices describe the ways individuals’ information may be used, shared and disseminated and provides prospective employees the opportunity to decline to provide personal information.

MySupport has undergone a formal Assessment and Accreditation and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. MySupport is rated as Moderate based on the type of data and it requires the Moderate baseline of security and privacy controls to protect the confidentiality, integrity and availability of the PII contained in the system. MySupport has developed a System Security and Privacy Plan (SSPP) based on NIST guidance and is a part of the FWS Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with DOI policy and standards.

Finally, the use of MySupport is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each account accessing the system; time and date of access; and activities that could modify, bypass or negate the system's security controls. Audit logs are encrypted and are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning are reported to the DOI Computer Incident Response Center (CIRC). FWS follows the principal of least privilege so that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete annual security and privacy awareness training, and those employees authorized to manage, use, or operate a system are required to take additional Role Based Security and Privacy Training. All employees are required to sign annually the DOI Rules of Behavior acknowledging their security and privacy responsibilities.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The data in MySupport is necessary to receive, track and process various administrative functions for FWS including hiring and payroll actions.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No – not applicable.

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable – no new data will be derived and placed in an individual's record with MySupport.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

User access is determined by what group/s the user belongs to and what role the user performs in the system, also known as Role Based Access Control. Using the principle of least-privilege, users are given access only to what they need to perform their official duties. Access to MySupport must be requested and approved by system administrators.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

FWS' MySupport contract is included under a DOI Interior Business Center contract which includes the required Federal Acquisition Regulation (FAR) clauses for privacy.

□ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

□ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

As part of information system security requirements an audit trail is enabled. The audit trail collects who logged in and from where and what actions were taken. All users of DOI computer systems and networks are notified that their activity may be subject to monitoring.

□ No

L. What kinds of information are collected as a function of the monitoring of individuals?

MySupport implements all NIST SP-800-53 Revision 4, Security applicable controls including the AC Access Control family and the AU Audit and Accountability control family. Audit logs capture: Date and time of the event, User ID and associated point of physical, Type of event, Names of resources accessed, and Success or failure of the event. The events audited include: Logon/off, both to the system and to the application, Failed authentication attempts, Resource access attempts that are denied by the access control mechanism, Privileged user actions, Activities that require privilege, All attempted accesses of security related resources, whether successful or not, Creation or deletion of users, Changes to user security information or access rights, Changes to system security configuration, Changes to system software, Attempts at escalation of privileges.

M. What controls will be used to prevent unauthorized monitoring?

All applicable controls from NIST 800-53 control families, AC - Access Control, IA - Identification and Authentication have been implemented. MySupport and its modules implement role based access control, using the principles of least privilege, where only users assigned to a role will have a specific set of permissions regarding the data they can access. Only system administrators have unrestricted access. Users are identified through the use of their FWS Active Directory account. There is no anonymous access. Users must use their FWS Active Directory account and PIV card to access MySupport which has been configured for single-sign on. System administrators are the only users that have access to audit data as it resides on system servers and enterprise log aggregation tools. Two-factor authentication is required to login to system servers, and only system security personnel are allowed access to log aggregation tools. Remote sessions to system servers are encrypted. All system traffic between the user and system is encrypted in accordance to NIST and DOI standards. The server hardware is managed and maintained within a secure network environment by the FWS Information Resources and Technology Management and there is no external access.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☒ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site

☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The MySupport Information System Owner is the official responsible for the oversight and management of the MySupport security controls and protection of information processed and stored by MySupport. The Information System Owner and the Information System Security Officer, in consultation with implicated Privacy Act System Managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy and providing adequate notice, making decisions on Privacy Act requests for notification, access and amendment, as well as processing complaints, in consultation with DOI Privacy Officials. These officials and authorized MySupport personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act and other Federal laws and policies for the data managed, used, and stored by MySupport.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The MySupport Information System Owner is responsible for oversight and management of the MySupport security and privacy controls, and for ensuring to the greatest possible extent that DOI and customer agency data in MySupport is properly managed and that access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and established procedures. In accordance with the Federal Records Act, the Bureau Records Officer is responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.