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: **Cost and Performance Management System (CPMS)**
Bureau/Office: **Fish and Wildlife Service (FWS)**
Date: **February 25, 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

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 Cost and Performance Management System (CPMS) is a system comprised of Commercial-off-the-Shelf (COTS) and custom developed applications integrated together to deliver functionality in two major areas: Cost and Performance Management and Human Capital Management. The Human Capital Management System (HCMS) is a submodule within CPMS and is comprised of a suite of automated human resources tools.

CPMS is an activity-based costing system that provides direct tracking of labor and operations costs, allowing visibility into full cost of mission activities and programs support. CPMS is able to trace all expenses and every hour of work back to the respective programs and hundreds of activities carried out in the various programs subcategories. CPMS provides the ability to develop performance models aggregating enterprise performance data as it relates to the FWS Operations Plan, Agency Priority Goals, Youth Hiring Initiatives, and future models as needed. CPMS also serves as an analytics platform providing ad-hoc and static reporting capabilities, dashboarding, and delivering notifications, giving FWS the ability to automate the population of performance tables used in developing the FWS Budget.

HCMS is comprised of four applications: the Workforce Planning Dashboard (WPD); Organization Chart Express (OCX); Position Description (PD) Express; and Job Announcement Express. HCMS uses data extracted from DOI's Federal Personnel and Payroll System (FPPS) and FWS' Corporate Master Table to provide managers with instant access to their workforce demographics via WPD. OCX automates and streamlines the process of developing and maintaining organizational charts and visualizing the FWS Organizational Hierarchy. PD Express allows managers to create and store positions descriptions, and Job Announcement Express allows managers to create and store job announcement components. PD Express and Job Announcement Express were developed to support OPM's End-to-End Hiring initiative.[1]

C. What is the legal authority?

Legal authorities include the following:

- Government Performance and Results Act of 1993
- 5 U.S.C. 3
- 31 U.S.C. 11
- 5 U.S.C. 5101, et seq.
- 31 U.S.C. 3512

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*

[1] See OPM's guidance on "End to End Hiring" at https://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/reference/end-to-end-hiring-initiative.pdf.

E. Is this information system registered in CSAM?

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

010-000000402; Cost and Performance Management System 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.*
Human Capital Management System ● PD Express ● Workforce Dashboard ● Organization Chart Express ● Job Announcement Express	Automate HR processes	Yes – Federal personnel only	Name, Employment Information, Military Status and FPPS Employee Common ID, Work email address (the same PII as CPMS). HCMS is a module within CPMS and shares same server and databases and leverages CPMS COTS software.

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)*

INTERIOR/DOI-85 – Payroll, Attendance, Retirement, and Leave Records (July 19, 2018) 83 FR 34156 and INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007) 72 FR 11040.

☐ 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 ☒ Employment Information ☒ Military Status/Service
☒ Other: *Specify the PII collected.*

FPPS Employee Common ID and Work Email Address. Employment information is limited to occupational series, grade, and entrance and/or separation date/s.

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*

DOI's FPPS is the source of the PII in CPMS.

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

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

The DOI FPPS is the source of the PII. Data is loaded as a flat file extract that is manually pulled from FPPS.

☐ Other: *Describe*

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

The intended and authorized uses of the PII collected in CPMS are to allow managers to plan for the retirement and recruitment needs of their workforces. Specifically, work email address is used to tie a user to an account in Active Directory for the purposes of authentication to the system. The "userPrincipalName" attribute of Active Directory is equal to an employee's work email address. Employee Common ID is a system generated identifier in FPPS and is used to uniquely identify an individual within the CPMS in order to tie employee activities to FWS financial data and personnel data from FPPS. Military Status and Employment Information as it relates to position (Work Schedule, Occupational Series, etc.) are used to stratify data for reporting purposes and are presented only at an aggregate level.

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.*

In the ordinary course of business, CPMS does not share PII. However PII may be shared with FWS personnel who have a 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 not routinely shared with other bureaus and offices. It is permissible to share PII from CPMS with authorized DOI personnel who have a need-to-know in the performance of their official duties.

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

PII is not routinely shared with external agencies. However, PII may be shared with other Federal agencies in accordance with the routine uses outlined in the INTERIOR/DOI-47 and INTERIOR/DOI-85 SORNs, including but not limited to: DOJ, including U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court and DOI is a party or has an interest in such litigation; Department of Treasury as required for payroll purposes; the Office of Personnel Management in connection with programs administered by that office; or to another Federal agency to which an employee has transferred. All DOI and FWS SORNs are available at https://www.doi/gov/privacy/sorn.

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

To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law--criminal, civil, or regulatory in nature.

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

Contractors are involved with development support and have limited access to CPMS data or PII; it is permissible to share PII with DOI "experts, consultants, grantees, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system" and have need to know in the performance of their official duties in accordance with the applicable routine uses in INTERIOR/DOI-47 and INTERIOR/DOI-85 SORN.

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

PII is not routinely shared with third parties but is permissible as outlined in the applicable routine uses in INTERIOR/DOI-47 and INTERIOR/DOI-85 SORNs.

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.*

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

CPMS does not collect PII directly from the individual so the system does not provide the individual an opportunity to decline to provide, or to consent to the use, of his or her PII. Instead, individuals have the opportunity to consent to the collection and uses of their PII during the onboarding process. They may decline to provide all the PII requested; however, this may prevent them from being able to onboard as FWS employees or contractors and perform their official duties.

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.*

Privacy Act Statements are provided to Federal employees during the onboarding process on the Declaration for Federal Employment, Employment Eligibility Verification and Fair Credit Reporting Release forms that are maintained in FPPS.

☒ Privacy Notice: *Describe each applicable format.*

Federal personnel receive notices of monitoring upon logging onto U.S. Government computers and systems.

☒ Other: *Describe each applicable format.*

This PIA, the FPPS PIA, and SORNs INTERIOR/DOI-47 and INTERIOR/DOI-85 provide further notice. Also see DOI instructions for requesting records protected by the Privacy Act at https://www.doi.gov/privacy.

☐ None

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

CPMS uses Employee Common ID for data processing on the backend and to positively match records with correct account. Employee Common IDs are only accessible to authorized system developers and administrators. System users have no direct access to CPMS' backend and cannot view the system's PII. Instead, users may create ad-hoc reports that display aggregate data – no PII - after providing their network credentials.

I. Will reports be produced on individuals?

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

☒ No

CPMS authorized users can create reports related to workforce planning and broad FWS performance measures. This data is in aggregate and does not contain PII or identify any specific employees or contractors.

Section 3. Attributes of System Data

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

No data will be collected from sources other than DOI records and systems.

B. How will data be checked for completeness?

Data is loaded from an extract from FPPS using an automated Extract Transform and Load (ETL) process. Any errors generated during the load process will be logged and investigated to ensure that the data loaded completely. System cannot correct for any errors propagated from FPPS. FPPS data verification procedures are described in the FPPS PIA available at https://www.doi.gov/privacy.

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

Data is manually extracted from the FPPS Datamart to flat files and loaded on a bi-weekly basis using automated ETL processes. FPPS data verification procedures are described in the FPPS PIA available at https://www.doi.gov/privacy.

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

CPMS records are considered temporary and maintained for 3 years in accordance with the Department's Administrative records schedule (DAA-0048-2013-0005) Short Term Human Resources Records.

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

Records are disposed of by 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.

The level of privacy risk to DOI personnel from collecting and using their PII in order to track labor and operations costs in CPMS is minimal. This privacy risk level is commensurate with the amount and type of PII in the system: name, military or veteran status, occupational series, grade and entrance/separation dates, FPPS Employee Common ID and work email address of Federal employees and contractors.

The primary risks to privacy are posed from unauthorized access and misuse of the data in the system. There is also a risk that individuals are unaware how their PII may be used within and shared outside of CPMS due to lack of system notice; however, all personnel are provided the opportunity to consent to the Department's collection, uses and sharing of their PII and other Privacy Act protected information during the onboarding process. Privacy risks from unauthorized system access and misuse of the data are mitigated by authenticating all users and controlling access. CPMS and its modules implement role-based access control using the principles of least privilege and limiting access to CPMS backend data to system administrators. Standard users are not granted access to PII and can only view CPMS data at the aggregate level.

Other potential privacy risks like maintaining unnecessary PII or data inaccuracies are mitigated by collecting only PII that is relevant to the system's purpose and by sharing data between FPPS and CPMS through flat file data extracts. Files are stored temporarily on the system, where only system administrators have access. Automated ETL processes are used to load the data into system databases. Error handling is incorporated in ETL processes to notify system administrator should processes fail. Upon completion of processing, all flat files are deleted. PII is used for internal processing and accessible by authorized administrators and developers; end users see data at an aggregate level and are unable to see it at an individual level. Also, instead of using PII that is sensitive on its own, such as SSNs, CPMS uses Employee Common ID to retrieve individual records.

CPMS 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. CPMS 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. CPMS 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 CPMS 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 DOI 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 information is needed in order to comply with Departmental requirements and the GPRA which requires bureaus to align funding to performance and mission activities. In addition, the HCMS modules were developed in-line with the President’s Management Agenda[2], to increase

[2] https://www.whitehouse.gov/omb/management/pma/

transparency into the hiring process to make it easier to attract and retain the best people; E-Government Act & Office of Personnel Management's End to End Hiring Initiative.[3]

☐ 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

Not applicable.

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

Not applicable.

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.*

[3] https://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/reference/end-to-end-hiring-initiative.pdf

☒ 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?

Using the principle of least-privilege, users are only given access to what they need. Access to CPMS and its component modules is determined using Role Based Access Control, where users are assigned to a role according to what role they need to perform in the system. Roles and responsibilities have been documented in the CPMS Standard Operating Procedures, Appendix T4. Only system administrators have access to all data. No other user roles are given access to data at a non-aggregated level.

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?*

CPMS is based off of an order from a GSA Schedule contract which includes the required Federal Acquisition Regulation (FAR) clauses for privacy: FAR 52.224-1-3 and 52.239-1.

☐ 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, audit logging is enabled in the systems which collect who logged in and from where, and what actions were taken while logged in. 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?

CPMS implements all NIST SP-800-53 Rev4 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 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. CPMS 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 not granted record level access to the data and are only able to view it at an aggregate level. 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 CPMS 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. Additionally, all system traffic between the user and system is encrypted via Secure Socket Layer technology. 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 CPMS Information System Owner is the official responsible for the oversight and management of the CPMS security controls and protection of information processed and stored by CPMS. The Information System Owner, Information System Security Owner, and the CPMS

Privacy Act System Manager 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 CPMS 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 CPMS.

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 CPMS Information System Owner is responsible for oversight and management of the CPMS security and privacy controls, and for ensuring to the greatest possible extent that DOI and customer agency data in CPMS 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, as well as the Federal customer agency, 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.