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: Environmental Conservation Online System (ECOS) or "ECOSPHERE"
Bureau/Office: U.S. Fish and Wildlife Service
Date: June 18, 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?

ECOS provides a central point of access to data regarding threatened and endangered species and conservation of wildlife habitats for approximately 50,000 users from Federal, Tribal, state, and local governments, non-government organizations (NGOs) and private institutions. The mission of the U.S. Fish and Wildlife Service (FWS or the Service) is to work with others to conserve, protect, and enhance fish, wildlife, plants and their habitats for the continuing benefit of the American people. ECOS contributes to this mission by facilitating the collaborative

administration of a network of national lands and waters among public and private partners for the conservation, management, and where appropriate, restoration of fish, wildlife and plant resources and their habitats within the U.S.

Some ECOS data is publicly accessible on the ECOS Homepage, such as Species and Critical Habitat Reports and Petitions to FWS. Other ECOS data is secure and requires a user account to access. For example, development projects subject to 50 CFR § 402.12 must be reviewed by FWS. Project proponents must create a user account and submit their project plans through the ECOS module Information for Planning and Consultation (IPaC) to ensure considerations for impacted threatened and endangered species are adequate.

ECOS is currently undergoing modernization and will transition into "ECOSPHERE" beginning in March 2020. ECOS will continue to be maintained throughout the transition period which is estimated to take five years. Instead of operating as a system of 37 different interconnected modules, submodules and web applications, the system will be developed using a data first architecture. This architecture will enable ECOSPHERE users to query from all of available data without having to login to different modules. Users will be authenticated by login.gov and then be granted access to data they are authorized access based on their user account roles and privileges. The Login.gov PIA is available on the General Services Administration website at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

This privacy impact assessment (PIA) will cover the ECOS and ECOSPHERE systems. "ECOS" will be used throughout the PIA to refer to both ECOS and ECOSPHERE unless explicitly differentiated.

C. What is the legal authority?

- Endangered Species Act of 1973 (16 U.S.C. 1531-1544), 50 CFR 17;
- Fish and Wildlife Coordination Act (16 U.S.C.661 et. seq., as amended);
- Estuaries and Clean Waters Act of 2000 (P.L. 106-457)
- Bald and Golden Eagle Protection Act (16 U.S.C. 668), 50 CFR 22;
- Migratory Bird Treaty Act (16 U.S.C. 703-712), 50 CFR 21;
- Marine Mammal Protection Act of 1972 (16 U.S.C. 1361, et. seq.), 50 CFR 18;
- Wild Bird Conservation Act (16 U.S.C. 4901-4916), 50 CFR 15;
- Lacey Act: Injurious Wildlife (18 U.S.C. 42), 50 CFR 16;
- Convention on International Trade in Endangered Species of Wild Fauna and Flora (TIAS 8249), http://www.cites.org/, 50 CFR 23;
- Coastal Barrier Resources Act (16 U.S.C. 3501 et seq., as amended).

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*

010-000000406; Environmental Conservation Online System (ECOS) System Security and Privacy Plan

TBD – ECOSPHERE is in the process of CSAM registration.

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

ECOS is undergoing modernization and will transition from operating as a system of 37 different interconnected modules, submodules and web applications into one "data lake." PII from the following ECOS subsystems will be available in ECOSPHERE.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Contaminants Assessment Process (CAP)	CAP is a standardized, ecological risk-assessment process for documenting and assessing threats posed by environmental contaminants to FWS lands and resources.	Yes	Contact information for members of the public who are interviewed by FWS in regard to environmental contamination issues.
Contaminants Investigation Database (CID)	CID is a legacy module that contains evaluations and approvals of proposed investigations into environmental contaminants.	Yes	Contact information for FWS employees and representatives of associated consulting firms.
Environmental Contaminants Data	ECDMS is a catalog of samples tested for	Yes	Contact information for non-Federal

Management System (ECDMS)	environmental contaminants.		government employees partnering with FWS.
Environmental Conservation Online System (ECOS) Common	ECOS is a gateway website that provides access to data from Ecological Services, Fisheries, and Refuges as well as other FWS and publicly available government data sources.	Yes	Username (email address) and password for non-Federal personnel; Active Directory login for DOI personnel and email address of other Federal agency personnel.
Injury and Mortality Reporting System (IMR)	IMR is an online application for tracking injury and death of Migratory Bird Treaty Act species	Yes	Contact information for individuals who submit responsive data.
Information for Planning and Consultation (IPaC)	IPaC provides a means for Project Proponents (pursuant to 50 CFR 402.12) to consider threatened and endangered species when evaluating the potential impacts of a project as required by law.	Yes	Contact information for project proponent points of contact, including Federal and non-Federal employees.
Monarch Conservation Data Application (MCD)	MCD collects information regarding efforts implemented to benefit monarch butterflies or their habitat to inform the decision on whether or not to list monarch butterflies as an endangered species.	Yes	Contact information for individuals who submit responsive data.
Tracking and Integrated Logging System (TAILS)	TAILS is a comprehensive activity-tracking system for Ecological Services Field Offices, who use the application to track and log workload and support annual performance reporting.	Yes	FWS employee username and password.

Threatened and Endangered Species System (TESS)	TESS manages and tracks data related to endangered species work including legacy and historical actions.	Yes	May contain FWS employee and/or member of the public's contact information from litigation proceedings, petitions, Federal Register notices, court and administrative decisions, Candidate Conservation Agreements, or Habitat and Conservation Plans.

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)*

ECOS is not a Privacy Act system of records. However, records for Federal user login are covered under the DOI system of records notice, INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) 72 FR 11040 (March 12, 2007). Records for non-Federal user login are covered under DOI system of records notice, INTERIOR/FWS-7, Water Development Project and/or Effluent Discharge Permit 73 FR 31877 (June 4, 2008). This SORN is currently under revision to provide general updates, including non-Federal user login information and access records, and to incorporate new Federal requirements in accordance with OMB Circular A-108. These SORNs may be viewed on the DOI SORN website at: https://www.doi.gov/privacy/sorn.

Records used to authenticate users through login.gov for ECOSPHERE are maintained under the GSA system of records notice, GSA/TTS-1, Login.gov, 82 FR 37451 (August 10, 2017) which may be viewed on the GSA SORN website at https://www.gsa.gov/reference/gsa-privacy-program/systems-of-records-privacy-act/system-of-records-notices-sorns-privacy-act.

☐ No

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

☐ Yes: *Describe*

☒ No.

ECOS maintains data that was collected under various OMB control numbers but the system itself is exempt from PRA; applicable OMB control numbers for ECOS data include:

1018-0023, Migratory Bird Surveys, 50 CFR 20.20; reapproval currently pending at OMB
1018-0158, Policy for Voluntary Prelisting Conservation Actions; expires 9/30/20
1018-0095, Endangered and Threatened Wildlife, Experimental Populations, 50 CFR 17.84; expires 12/31/20
1018-0148, Land-Based Wind Energy Guidelines; expires 11/30/21
1018-0119, Policy for Evaluation of Conservation Efforts When Making Listing Decisions (PECE); expires 6/30/21
1018-0162, Management of Non-Federal Oil and Gas Rights, 50 CFR 29, Subpart D; expires 11/30/22
1018-0165, Revisions to the Regulations for Petitions, 50 CFR 424.14; reapproval currently pending at OMB

All FWS Information Collection packages may be queried on OMB's Information Collection Dashboard at https://www.reginfo.gov/public/jsp/PRA/praDashboard.myjsp.

Section 2. Summary of System Data

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

☒ Name ☒ Personal Cell Telephone Number ☒ Personal Email Address
☒ Group Affiliation ☒ Home Telephone Number Status ☒ Mailing/Home Address

☒ Other: *Specify the PII collected.*

Business or affiliation phone numbers, mail and email addresses, username and password including Active Directory (AD) login for DOI/FWS personnel.

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
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*

ECOS shares permits data with FWS' permitting system.

☐ Other: *Describe*

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

The intended use of the PII collected is to access data in ECOS regarding threatened and endangered species and conservation of wildlife habitats. Usernames, email addresses and passwords are collected in order to grant authorized access to the system. Contact information is collected to facilitate communication among conservation partners and FWS.

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.*

ECOS PII may be shared 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.*

☐ 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.*

ECOS PII may be shared with FWS contractors who have need-to-know in the performance of their official duties.

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

Contact information may be shared among ECOS users, including NGO's and individual members of the public, who participate in the same collaborative program/s or project/s, and/or

have provided consent to share their contact information with other ECOS users. For example, the Iowa Department of Natural Resources partners with FWS to monitor monarch butterfly habitats in the state. The Iowa Department of Natural Resources may, with the individual's consent, share another Monarch Conservation Data (MCD) user's contact information with personnel from the University of Iowa for the purposes of collaboration on conservation efforts.

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.*

Individuals may decline to provide their PII and will not be able to create a user account or access ECOS. The ECOS account creation and login pages contain the required Privacy Act statements and privacy policy providing users notice of all permissible uses and sharing of their PII and that providing the PII is voluntary but necessary in order to access ECOS.

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

ECOS does not provide an opportunity to FWS employees and contractors to decline to provide information or to consent to the specific uses of their information; however, they are provided notice as to how their PII will be used and shared in order to perform their jobs during the hiring and onboarding process.

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 Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the GSA login.gov PIA, and related SORNS published in the *Federal Register*. The ECOS and IPAC login pages contain a privacy notice. 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 on the ECOS and IPaC login pages that informs them 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.).

User roles and account privileges are retrieved by the username or Active Directory login for DOI users in order to grant authorized access to ECOS; otherwise personal identifiers are not used to retrieve ECOS records or data.

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?

PII of non-Federal users is verified through the user account creation and verification process. ECOS program managers (FWS employees) must approve all new user account requests. Once approved the ECOS helpdesk sends an automated email message to the user with instructions on how to complete setting up his or her account. Email addresses that are incorrect will be unable to receive the account approval message and will not be able to create a user account until a correct email address is provided.

B. How will data be checked for completeness?

The account creation form utilizes required fields to ensure complete submissions; users who do not complete each required data field cannot create an ECOS user account.

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

ECOS sends reminders to users to update their account passwords every 90 days. This provides individuals regular opportunities to review and modify their contact information as necessary. IPaC also sends periodic emails to users requesting they change their passwords and validate their contact information. Otherwise it is the user's responsibility to provide necessary updates to their contact information. Users may access their account profiles at any time in order to review and modify their contact information.

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

ECOS user access account records are considered temporary and may be maintained for a maximum of three years in accordance with the Department's Records Schedule for Short-term Information Technology Records 1.4.A. "Active" accounts are retained indefinitely, provided that the user updates his or her password every 90 days. Accounts that are inactive for 90 days are disabled.

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.

The privacy risk to users of ECOS is considered moderate. The primary privacy risks are from potential unauthorized access, use, and disclosure of PII in the system. Other privacy risks posed by the maintenance of PII in the system are: users may not be fully aware of the extent to which their PII may be disclosed outside of the Service, and maintaining inaccurate PII in the system. These risks are mitigated by a variety of administrative, technical and physical controls and best practices.

Only authorized individuals are granted system access to ECOS. FWS employees who serve as program and/or application managers must approve all new user requests. Access to data within ECOS is further protected from unauthorized access by the specified roles and privileges of the user account. Users can only access data for programs and projects in which they are participating or overseeing. Users receive periodic reminders to change their passwords and update their user profiles to help only accurate information is maintained. Accounts that are for at least 90 days are deleted.

Users also receive privacy notices and acknowledge by logging in that they are subject to monitoring of the system for lawful, authorized and appropriate use. Federal users of ECOS must complete annual security and privacy training, acknowledge their roles and responsibilities with regard to security and privacy by reading and signing the DOI Rules of Behavior. ECOS features an auditing trail which the System Administrator can use to identify any unauthorized access or change to the system.

ECOS collects the minimum PII necessary to authorize system use, grant access and facilitate communication among ECOS users and involves the individual in the process through the user

account creation and verification process. ECOS only collects contact information as well as username and password; ECOS does not collect any Sensitive PII. The use of GSA's Login.gov also helps to minimize the PII that FWS needs to collect for user authentication purposes. Privacy risks and mitigations for the use of Login.gov may be found in GSA's PIA at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

It is possible that a member of the public may be referred to FWS for potential participation in a collaborative project or study that utilizes ECOS without prior notification. In these cases, FWS encourages users and project partners to let the individual know that his or her contact information will be provided to the Service and that we may reach out to coordinate participation in a project. The Service does provide adequate notice of all the permissible uses and sharing of ECOS data with Privacy Act statements, website privacy policy notices, publication of this PIA and the INTERIOR/DOI-47 SORN in the *Federal Register*.

Finally, ECOS 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. ECOS 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. ECOS 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.

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*

ECOS collects the minimum PII necessary to allow for authorized access and use of the system, and for potential participation in a collaborative project or study that utilizes ECOS.

☐ 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

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. The system does not derive new data about individuals.

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?

ECOS program managers (FWS employees) must approve the creation of all ECOS user accounts. The process for requesting an ECOS user account varies: ECOS program managers may solicit a select body of biologists and researchers to provide information for certain studies. If these individuals agree, the ECOS Helpdesk will email them login instructions. Individuals

may contact FWS program managers directly when interested in participating or partnering with FWS.

Individuals subject to 50 CFR 402.12 must create IPaC accounts to define a project or request an official species list or may work directly with a FWS regional office. Once an individual creates an account, the ECOS Helpdesk (or IPaC) sends an email confirmation to help authenticate the individual's need and purpose for accessing the system.

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?*

The ECOS contract contains the required privacy clauses per Federal Acquisition Regulations.

☐ 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*

Audit logs, accessible only to system administrators with elevated privileges, provide the capability to identify users in the event of inappropriate usage; however, ECOS is not intended to identify, locate and monitor individuals.

☐ No

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

Systems and Application level event logging is enforced to monitor user account modifications and other events of interest. These logs include the system generated date and time stamp of the event, event type, event outcome, and associated usernames in accordance with NIST SP 800-53 Rev. 4 Control AU-03(1).

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

ECOS utilizes the concept of least access thus limiting access to the minimum functions necessary for the user to perform his or her official duties. Only system administrators who have elevated privileges may access the audit log in accordance with NIST's Control AU-09(4) Protection of Audit Information - Access by Subset of Privileged Users to help prevent unauthorized monitoring. This control requires that the number of users authorized to perform audit-related activity is limited to a small subset of privileged-users.

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 ECOS Information System Owner is the official responsible for the oversight and management of the ECOS security controls. The Information System Security Owner and the Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy. These officials and all authorized ECOS users and system administrators are responsible for protecting information processed and stored by ECOS and for meeting the requirements of the Privacy Act and other Federal laws and policies for the data managed, used, and stored by ECOS in consultation with the FWS Associate Privacy Officer. ECOS oversight and safeguards help to protect the privacy of the individuals about which information may be reside in ECOS.

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 ECOS Information System Owner is responsible for oversight and management of the ECOS security and privacy controls, and for ensuring to the greatest possible extent that DOI and FWS data in ECOS 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 Departmental Records Officer and bureau Records Officers are responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.