Appendix A: DI-4001 PIA Form

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: Eastern Population of Greater Sandhill Crane Fall Survey

Date: March 16, 2017

Bureau/Office: United States Fish and Wildlife Service (USFWS)

Bureau/Office Contact Title: Migratory Bird Management

Point of Contact
Email: dave_fronczak@fws.gov
First Name: David
M.I.: L
Last Name: Fronczak
Phone: 612-713-5411
Address Line 1: 5600 American Blvd., West
Address Line 2: Suite 990
City: Bloomington
State/Territory: MN
Zip: 55437

Section 1. General System Information

A. Is a full PIA required?
This is a threshold question. Indicate whether the system collects, maintains, uses or disseminates information about members of the general public, Federal employees, contractors, or volunteers. If the system does not contain any information that is identifiable to individual (e.g., statistical, geographic, financial), complete all questions in this section and obtain approval and required signatures in Section 5. The entire PIA must be completed for systems

that contain information identifiable to individuals, including employees, contractors and volunteers.

☒ 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?
Describe the purpose of the system and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.

The USFWS has coordinated a long-term fall survey of Eastern Population of greater sandhill cranes (hereafter, EP cranes) in the Mississippi and Atlantic Flyways, since 1979 for management purposes. This survey contributes to the monitoring of the status and regulates the harvest strategy of EP cranes. The survey is conducted annually at the end of October by volunteers and federal and state agency personnel. During the survey, the number of cranes at historic migratory staging areas is recorded, providing a fall index of the population. Personnel data of contributors conducting the survey is, in part, used solely for the coordination of the following year survey and to answer any questions pertaining to individual observations.

C. What is the legal authority?
A Federal law, Executive Order of the President (EO), or DOI requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.

- Migratory Bird Treaty Act
- Migratory Bird Conservation Act
- EO Order 13186, Responsibilities of Federal Agencies to Protect Migratory Birds

D. Why is this PIA being completed or modified?
Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.

☐ 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?
The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.
Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA. A separate PIA should be conducted for each hosted application or subsystem that contains PII to ensure privacy implications are assessed. In any case, the GSS PIA must identify all hosted applications, describe the relationship, and reference or append the PIAs conducted for the hosted applications. The GSS PIA and associated PIAs must be reviewed and approved by all officials as appropriate; and all related PIAs, SORNs and supporting artifacts must be entered into CSAM.

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)?
A Privacy Act SORN is required if the information system or electronic collection contains information about individuals that is retrieved by name or other unique identifier. Provide the DOI or Government-wide Privacy Act SORN identifier and ensure it is entered in CSAM for this system. For new SORNS being developed, select "Yes" and provide a detailed explanation. Contact your Bureau Privacy Officer for assistance identifying the appropriate Privacy Act SORN(s).

☒ Yes: *List Privacy Act SORN Identifier(s)* FWS-26
☐ No

H. Does this information system or electronic collection require an OMB Control Number?
The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to

determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.
Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

☒ Name	☐ Credit Card Number
☐ Citizenship	☐ Law Enforcement
☐ Gender	☐ Education Information
☐ Birth Date	☐ Emergency Contact
☐ Group Affiliation	☐ Driver's License
☐ Marital Status	☐ Race/Ethnicity
☐ Biometrics	☐ Social Security Number (SSN)
☐ Other Names Used	☒ Personal Cell Telephone Number
☐ Truncated SSN	☐ Tribal or Other ID Number
☐ Legal Status	☒ Personal Email Address
☐ Place of Birth	☐ Mother's Maiden Name
☐ Religious Preference	☒ Home Telephone Number
☐ Security Clearance	☐ Child or Dependent Information
☐ Spouse Information	☐ Employment Information
☐ Financial Information	☐ Military Status/Service
☐ Medical Information	☐ Mailing/Home Address
☐ Disability Information	
☐ Other: *Specify the PII collected.*	

B. What is the source for the PII collected? Indicate all that apply.
Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

☒ Individual   Personal contact information would be collected through a single source website provided by the individual (public volunteers, state or federal agency personnel). Personnel will have the choice of entering personnel contact information.
☐ 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.
Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.

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

D. What is the intended use of the PII collected?
Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.

The personal contact information of volunteers and state/federal agency personnel will be used for coordination purposes for the participation of the following year's survey. Personal contact information may also be used to contact individuals if there are any questions pertaining to the previous year's survey observation.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.
Indicate all the parties, both internal and external to DOI, with whom PII will be shared. Identify other DOI offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.

Appendix A – DI-4001 PIA Form

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.* The personal contact information of volunteers and state/federal agencies will be used solely by two survey coordinators within the Region 3, Migratory Bird Management program.

☐ 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.*

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

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?
If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
Individuals that enter observations within the survey website will have the option to fill in contact information if they choose.

☐ 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.
Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

Appendix A – DI-4001 PIA Form

☒ Privacy Act Statement: *Describe each applicable format.*
    Privacy Act Statement:
    Authority: The Migratory Bird Treaty Act (16. U.S.C 703-712), the Fish and Wildlife
    Improvement Act of 1978 (16 U.S.C. 7421) and the Fish and Wildlife Act of 1956 (16 U.S.C.
    742 a-j).
    Purpose: The purpose for collecting the contact information is to coordinate EP Crane
    Survey volunteers for participation in current and possibly future surveys. This monitoring is
    conducted annually and helps in the management of the harvest strategy for EP Cranes.
    Routine Uses: The contact information of the volunteer may be used to inquire about survey
    observations and/or for participation in future surveys. Contact information will be shared
    with the Survey Coordinators within the Region 3, Migratory Bird Management Program.
    More information about the routine uses can be found in the systems of records notice,
    Migratory Bird Population and Harvest Systems, FWS-26.
    Disclosure: All information is voluntary. Individuals have the option to not provide contact
    information.

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☐ None:

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).
Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).

Users of the website will be required to enter a username and password to enter website. If personal contact information is provided by volunteer or state/federal agencies, that information will be stored within a secured database, maintained by the IRTM managers. If needed, personal contact information can be retrieved by (name/email) and will be accessible only by data managers and provided to survey coordinators, upon request.

I. Will reports be produced on individuals?
Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have features that allow reports to be generated on data in the system or on user actions within the system.

☐ 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 accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.

Personal contact information provided by volunteers and state/federal agencies will be verified by the individual entering information. Data is not collected from any other source.

B. **How will data be checked for completeness?**
Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.

Not applicable, personal contact information provided by volunteers and state/federal agencies will be verified by the individual entering information.

C. **What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).**
Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

Not applicable, personal contact information provided by volunteers and state/federal agencies will be verified by the individual entering information.

D. **What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.**
Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with Bureau/Office Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. Be sure to include applicable records retention schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.

Retention periods will be on a yearly basis. Personnel will be contacted, via contact information provided by individuals, and asked to participate with the survey for the following year. Some individuals may opt out of participating in the survey, which will determine if information is retained.
PROJ – 240 Statistical Information Files
PROJ – 600 Program Files

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?
Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, bureau/office records management policies, or standard operating procedures.

If the individual opts out of participating with the following year's survey, then the individual and their contact information will be removed from the database. There are no existing procedures for deleting contact information from database. However, it will be imposed by the USFWS survey coordinators to have IRTM managers confirm any requests to eliminate contact information from the database.

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.
Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the Department and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department.

Privacy risks with collecting volunteer and federal/state agencies personal contact information will be negligible, as it is non-sensitive personal information. And release of observer information from an EP Crane population survey will not result in harm to any party. Information is not shared outside of the Service. Access and identification and authentication controls are in place to prevent unauthorized access.

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?
Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information

about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.

☒ Yes: *Explanation* The personal contact information provided by volunteers and state/federal agency personnel who participate in the fall survey will allow USFWS, Migratory Bird Management coordinators to coordinate for the following year's survey and allow the opportunity to ask questions pertaining to an observation from a survey.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?
Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

☐ 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?
Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☒ No: Personal information provided by volunteers and state/federal agency personnel that participate with the survey will be contacted for the coordination for the following year's survey and if, the coordinator needs additional information about the previous observation.

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

Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?
Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

Not applicable, personal contact information provided by volunteers and state/federal agencies will be verified by the individual entering information. There is no new data.

F. Are the data or the processes being consolidated?
If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

☐ 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.
Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system? Also consider "other" users who may not be as obvious, such as

the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.

☐ Users
☐ Contractors
☐ Developers
☒ System Administrator   USFWS, website managers
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?
Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards [FIPS] Publications in the authorities section. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of applying logical access controls, which are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of information system owners to ensure no unauthorized access is occurring.

Access to data will be restricted for the use by the USFWS, Migratory Bird Management survey coordinator and access to data within the database will be restricted by the USFWS, website managers.

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?*

☒ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?
Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

☐ Yes. *Explanation*

☒ No

Appendix A – DI-4001 PIA Form

K. Will this system provide the capability to identify, locate and monitor individuals?
Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

☒ Yes. *Explanation* For auditing purposes, USFWS, Website managers will incorporate the capability to identify individuals who access the website.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?
The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) detail how audit logs should be used for DOI systems. Provide what audit activities are maintained to record system and user activity including invalid logon attempts and access to data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication of users to the system. Examples of information collected may include username, logon date, number of failed logon attempts, files accessed, and other user actions on the system.

Audit logs collect the username, result of access (granted/denied) and time and date of access.

M. What controls will be used to prevent unauthorized monitoring?
Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.

Individuals who participate with the survey and enter data into the website, will be required to create and username and password. The concept of least privilege is employed to limit access to authorized administrators. Access requires elevated privilege.

N. How will the PII be secured?
Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

Appendix A – DI-4001 PIA Form

(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.
Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public. For Privacy Act responsibilities refer to 383 Department Manual

Chapters 1-13 and DOI Privacy Act regulations at 43 CFR Part 2. Also, describe how Privacy Act complaints and requests for redress or amendment of records are addressed.

The FWS Associate Privacy Officer is responsible for protecting the privacy rights of the employees, contractors and the public whose information may be collected, stored or processed within FWS. The Privacy Officer is also responsible for addressing Privacy Act complaints or requests for redress.

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?
This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Head of the Bureau or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.

The USFWS, website managers and the USFWS, Migratory Bird Management survey coordinators will be responsible for the protection and unauthorized access of personal contact information provided by survey contributors. In addition, the information system owner and the privacy officer are responsible for assuring proper use of employee data. Loss, compromise, unauthorized disclosure or unauthorized access of PII is considered a "security incident" that must be reported to DOI-CIRC within one hour of discovery.

Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the DOI Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

Information System Owner

Email: Dave Fronczak
First Name: Dave   M.I.:   Last Name: Fronczak Title: Migratory Bird Management
Bureau/Agency: DOI/FWS   Phone: 612-713-5411   Date:

Signature:

Appendix A – DI-4001 PIA Form

Information System Security Officer

Email: john_g_herron@fws.gov
First Name: John   M.I.: G   Last Name: Herron   Title: RITSM
Bureau/Agency: DOI/FWS   Phone: 612-713-5116   Date: 6/6/2017

Signature:

Privacy Officer

Email: Katherine_gonyea@fws.gov
First Name: Katherine   M.I.: E.   Last Name: Gonyea   Title: Privacy Officer
Bureau/Agency: U.S. Fish & Wildlife Service   Phone: 703-358-2244   Date:

Signature:

Reviewing Official

Email: Kenneth_Taylor@fws.gov
First Name: Kenneth M.I.:   Last Name: Taylor   Title: Assistant Director of Information Resources
Bureau/Agency: U.S. Fish & Wildlife Service   Phone: 703-358-1968   Date:

Signature: