U.S. Fish & Wildlife Service
Privacy Program Handbook

(*Supplements 204 FW 1*)
April 2024

Table of Contents

Background

Congress passed the Privacy Act of 1974 to balance the need for Federal agencies to maintain information about individuals with the rights of those individuals to be protected from unwarranted invasions of their privacy.

The Department of the Interior (Department) privacy program is committed to fulfilling the requirements of the Privacy Act to the greatest extent possible. The main objectives of the Department's program are to:

1. Restrict disclosure of personally identifiable records maintained by the Department;
2. Grant individuals the right to access agency records maintained on them;
3. Grant individuals the right to seek amendment of agency records maintained on themselves upon showing the records are not accurate, relevant, timely, or complete; and
4. Establish a code of fair information practices requiring the Department to comply with statutory norms for collection, maintenance, and dissemination of records.

Purpose

The purpose of this handbook is to provide guidance to U.S. Fish & Wildlife Service (Service) Privacy Act System Managers, System Owners, Information System Security Officers (ISSO), and any other Service employee who may be involved with the creation, maintenance, dissemination, and protection of Personally Identifiable Information (PII). We based the guidance on requirements established by the Department, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB), and it is meant to complement and clarify the requirements and policy in 204 FW 1, Privacy Program, by providing more specific guidance for:

- Appropriately handling PII and Sensitive PII (SPII);
- Conducting and developing Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and other privacy documentation;
- Completing required privacy awareness training and Role-Based Privacy Training (RBPT); and
- Reporting confirmed or suspected privacy breaches.

The requirements in this handbook apply to all Service employees, contractors (through their contracts), volunteers, partners, and others who perform work for or on behalf of the Service. We use the term "employee" in this chapter as a general term to describe all of these individuals.

PII and SPII

PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to an individual. An individual's name does not have to be present for information to be PII. In addition, PII can be created when information about an individual is made available or combined with other information. Some examples include email addresses, phone numbers, photographs, license plate numbers, and logins or usernames.

Some PII is not sensitive, such as information found on a business card or in an official email signature block. This type of non-sensitive PII generally does not require special handling. However, there is also SPII, which if lost, compromised, or inappropriately disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual or the agency. Sensitivity of PII is in part determined by context, such as a list of employees with poor performance ratings as opposed to a list of employees who completed privacy training. Some examples include Social Security Numbers (SSN), credit card or financial account numbers, personal identification numbers, passwords, and more.

Regardless of sensitivity, employees must be careful when handling PII. Handling SPII requires additional care given the increased risk of harm to an individual if it is compromised. Chapter 3 defines handling requirements in more detail.

Chapter 1 – Program Management

Those responsible for the protection of people's privacy are scattered throughout the Service. This chapter briefly explains the different roles involved in managing the privacy program. For a full list of roles and responsibilities related to the Service's privacy program, see 204 FW 1. Chapter 204 FW 1 also provides additional requirements related to training, contracts, and assessments to ensure privacy is appropriately handled throughout all applicable activities.

Privacy Program Roles

The **Associate Chief Information Officer (ACIO)** is responsible for overseeing Information Management and Technology (IMT) functions for the Service. The ACIO has a critical role in assuring the security of Federal information and information systems and oversees the Service privacy and cybersecurity programs. The ACIO is the Assistant Director – Information Resources and Technology Management (IRTM).

The **Associate Chief Information Security Officer (ACISO)** is responsible for coordinating, developing, and implementing the Service's cybersecurity program. The Service ACISO works closely with the appropriate privacy and security staff in the program offices to review, evaluate, and recommend information security and privacy measures and safeguards to protect information from loss, theft, misuse, unauthorized access, destruction, and unauthorized modification or disclosure whether accidental or intentional.

The **Associate Privacy Officer (APO)** is responsible for managing and overseeing privacy activities to ensure compliance with Federal privacy laws and policies. The Service APO implements privacy policy; provides guidance; evaluates Service programs, systems, and initiatives for potential privacy implications; and provides strategies to mitigate or reduce privacy risk. The APO leads the Privacy Division (formally referred to as the "Associate Privacy Officer" in 142 Departmental Manual 14) within IRTM.

Privacy Act System Owners/Managers are the officials with administrative responsibility for managing and protecting Privacy Act records, whether in electronic or paper format, and for meeting the requirements of the Privacy Act and the published System of Records Notices (SORN).

The **Information System Security Officer (ISSO)** is responsible for collaborating with System Owners/Managers to develop, implement, and manage the systems they own and operate. The ISSO ensures that operational security is maintained and cybersecurity requirements are met.

Managers and supervisors ensure employees under their supervision complete mandatory annual privacy training, and, if required, Role-Based Privacy Training (RBPT) for employees with significant privacy responsibilities.

Employees are required to follow Service privacy policy, keep PII secure, and only disclose information to those with a need to know. All employees are required to complete the mandatory annual privacy training. Certain employees have significant privacy responsibilities and are required to complete RBPT and the self-certification acknowledging their responsibility for protecting PII.

Training

The Federal Information Security Modernization Act (FISMA) of 2002 requires each agency to provide basic security and privacy awareness training for Federal employees. OMB Circular A-130, Managing Information as a Strategic Resource, outlines the basic training requirement. It further mandates that agencies provide role-based security and privacy training to employees with assigned security and privacy roles and responsibilities before authorizing elevated access to Federal information resources or performing assigned duties. The training requirements for Service employees are as follows:

A. **Privacy awareness.** All employees who access the Department and Service network are required to complete the annual IMT Awareness Training to maintain network access. This training includes basic privacy awareness training, so all employees are familiar with the requirements for handling and protecting PII.

B. **Role-based training.** Employees with privacy roles and responsibilities are required to complete the annual RBPT and a self-certification acknowledging their responsibility to protect it. Employees to whom this requirement applies must complete this course to maintain network access. These employees include, but are not limited to: human resources professionals, law enforcement professionals, supervisors, and employees with access to systems that contain records protected by the Privacy Act. Role-based training is assigned by the Department. Changes to RBPT assignment must be coordinated between the Department, the Service Privacy Division, and the supervisor.

C. **Requested training.** The Privacy Division within IRTM can provide additional training upon request. Offices may request training by emailing FWS_Privacy@fws.gov if they feel their group might benefit from a privacy presentation and the opportunity to ask questions.

Chapter 2 – Important Federal Privacy Concepts

This chapter covers certain key privacy concepts introduced in 204 FW 1 in greater detail, including the relationship between the Privacy Act of 1974, the E-Government Act of 2002, and the Paperwork Reduction Act. These three laws provide the baseline requirements the programs, offices, and employees must consider when creating, maintaining, disclosing, or taking any other actions with PII or other information subject to the Privacy Act. This guidance is not intended to replace Departmental or Service privacy training or directives.

The Privacy Act of 1974 and Systems of Records

The Privacy Act of 1974 applies to information about an individual contained in an agency system of records. The Privacy Act requires agencies publish a System of Records Notice (SORN) describing specified aspects of the system, including the individuals covered, the records you maintain about those individuals, and to whom you disclose information about those individuals.

"System of records” is a term of art that covers systems where you retrieve information by a person’s identifier. For example, if you retrieve data from a system by searching for an identifier such as name, ID number, or permit number, you may be operating a system of records and the requirements of the Privacy Act will apply. However, if you retrieve data by searching for a calendar date or company, you may not be operating a system of records.

The basic rule in the Privacy Act is that you may not disclose information from a system of records unless the individual has consented in writing. The information need not actually be private. An individual’s name, by itself, may be protected information. Information readily found in a phone book or other public source may be protected, as well as information that an individual may have posted on a website or other public forum. The key is whether the information comes from a system of records and relates to an individual, including a unique personal identifier assigned to the individual.

Exceptions to this rule are discussed in the “Privacy Act Requests and Disclosures” section of Chapter 3. For example, you may disclose information to Departmental employees when they need the information to perform their duties, and you may disclose information under a published routine use as designated in the applicable SORN. If you are uncertain about whether you are operating or can provide information from a system of records, consult with the Service’s Privacy Office.

E-Government Act of 2002 and Privacy Impact Assessments (PIA)

The requirements of the E-Government Act of 2002 apply to all information in identifiable form, making it broader than the Privacy Act because it applies to any information about an individual, whether you keep it in a system of records or not. The main requirement of the E-Government Act is that we must conduct a Privacy Impact Assessment (PIA) on any information system that maintains or disseminates information in identifiable form on members of the public. We must conduct a PIA prior to operating the system or update it prior to making any significant changes. Chapter 4 provides more information on PIAs.

Paperwork Reduction Act (PRA) and Information Collections

The PRA applies to collections of information from 10 or more non-Federal individuals or entities (including local, State, and Tribal governments). The “10 or more” rule is irrelevant for any requirement contained in a rulemaking or if it is addressed to all or a substantial majority of an industry (e.g., if there are only five main companies in a particular industry). It applies regardless of whether the collection is voluntary or whether the collection is written or verbal or collected electronically or via hardcopy forms/documents. The PRA imposes restrictions on these collections by requiring us to work with OMB to obtain a control number indicating that we have permission to collect the information. In accordance with 281 FW 4 and 281 FW 5, the Service’s Information Collection Clearance Officer (ICCO) must review all proposed applications or systems that will collect information from the public to determine whether the collection will need further review from OMB.

Privacy Act and Information Collection

The Privacy Act also requires us to provide a Privacy Act statement when we collect information directly from an individual. The Privacy Act statement (“e3 statement”) explains why you are collecting the information, how you will use it, whether it is mandatory, and any consequences for failing to provide it. The Service’s privacy program can help you draft it, or you can review the Department’s training on the subject for more information. If your program collects PII that is not maintained in a system of records, like a refuge visitor’s home zip code for a survey, you should still provide a basic notice to the individual regarding how their PII may be used or disclosed.

Other Considerations

Some other important privacy considerations and concepts include:

- SORNs, PIAs, and OMB control number requests all take time to complete, especially if you do not know exactly how your program will work.
- Willful violations of the Privacy Act can be punished both civilly and criminally. The courts have interpreted “willful” to include not just intentional violations, but also disclosures of information in flagrant disregard of the Privacy Act or without grounds for lawful disclosure.
- Think about to whom you are disclosing information. Don’t copy a second-tier manager on an email that includes an individual’s name, SSN, or date of birth if that second-tier manager really

doesn't need the information. Password-protect attachments that have lists with PII. See Chapter 3 for more information.

Chapter 3 – Privacy Requirements

Protecting PII and Privacy Act Information

Employees must implement the following requirements to protect Privacy Act information, PII, and SPII:

A. **Need to know**. Only disclose or share information from a system of records within the Department to those who have a need to know to perform their official duties. This handbook provides information on disclosure and sharing beyond the Department below. While not necessarily explicitly protected by the Privacy Act, SPII is a policy-based categorization of information the Department requires us to protect regardless of whether it is part of a Privacy Act system of records or not. To be safe, the best practice is to handle all PII like it is protected by the Privacy Act and only disclose or share it within the Department to those who have a need to know.

B. **Physical security.** Physical PII must be stored in a secure location (e.g., locked drawer, cabinet, or safe) when not in use or under the control of a person with a need to know. PII may be stored in a locked room or an area where access is controlled by a guard, cipher lock, or card reader that prevents unauthorized access by members of the public, visitors, or other people without a need to know. Privacy Act information may also be marked with: "Warning: Disclosure controlled under the Privacy Act of 1974 (5 U.S.C. 552a)."

C. **Shared drives.** Store PII in shared access computer drives only if access is restricted to those with a need to know by permissions settings or passwords. Owners of PII on network drives, shared network drives, and collaboration systems including, but not limited to, SharePoint, One Drive, and Teams are required to ensure appropriate security and privacy controls are in place to limit access to authorized users and to encrypt folders, when possible, if there is an official need to post PII to those systems. Owners of PII on shared network drives and collaboration systems should conduct audits of these systems on at least an annual basis to review and verify authorized user access and the continued need for maintaining PII on the system.

D. **Personally-owned equipment.** Departmental policy forbids using personally-owned equipment to access, save, store, or host PII. In addition, personal email accounts may not be used to transmit any PII. See IT Bulletin 2023-002 for more information on restrictions on personally-owned equipment within the Service.

E. **Protections for SPII.**

- **a.** **To protect SPII do not:**
    - i. Leave your PIV card unattended in your computer. Log off, turn off, or lock your computer whenever stepping away to ensure no SPII is compromised.
    - ii. Discuss or entrust SPII to anyone who does not have a need to know. Be conscious of the environment and your surroundings when discussing SPII.
    - iii. Send SPII to a fax machine without contacting the recipient to arrange for its receipt.
    - iv. Store, access, save, or process SPII on personally-owned equipment.
    - v. Take SPII to your home or to any non-Departmental worksite, in either paper or electronic format, unless authorized by your supervisor or manager and appropriately secured using either encryption (if electronic) or by locking it in a container.

b. **Storage.** Use only approved, Government-furnished equipment such as desktops, laptops, and removable storage media (e.g., external hard drives, flash drives, and memory cards) to store SPII. These devices must be secured with authorization and encryption mechanisms or equivalent protection. See IT Bulletin 2022-006, Requirements for Using Removable Storage Media, for more information on encryption requirements for removable storage media.
c. **Destruction of SPII.** Destroy all SPII when it is no longer needed and continued retention is not required per the applicable records schedule. Destruction may be accomplished by shredding, burning, or through other means to make the SPII irretrievable in accordance with National Institute of Standards and Technology (NIST) guidelines. See the Disposing of SPII section below.
d. **Breaches.** Immediately report any suspected or confirmed loss, theft, or unauthorized disclosures of SPII to your supervisor or Program Manager, the Service's privacy program (FWS_Privacy@fws.gov), the Service's Security Operations Center (FWHQ_IRTM_Security@fws.gov), and the Department's Computer Incident Response Center (doicirc@ios.doi.gov). See Chapter 5 for more information.

Transmitting PII

The following requirements apply for transmitting PII via email, mail, or other methods.

A. **Physical security.** Physically secure PII when in transit. For example, do not pack laptops or removable storage media in checked baggage. Do not leave physical copies of PII in a car overnight or in plain sight in a parking lot. Do not mail or courier sensitive PII on CDs unless the CD is encrypted.

B. **Mailing PII.**

a. **Mailing PII within the Department.** Mail PII in an approved messenger envelope provided by your office or mailroom. Be sure to encrypt PII transmitted on CDs, flash drives, or other removable storage media, and apply appropriate Controlled Unclassified Information (CUI) markings.
b. **External mail.** Seal PII in an envelope, double wrap contents, and tape both ends of the envelope. Mark the inner envelope with appropriate CUI markings and warning labels. Be specific about the sender and recipient so mail room or administrative personnel do not need to open the envelope to deliver it. Use First Class or Certified Mail with tracking capability or a traceable commercial delivery service (e.g., UPS or FedEx). Encrypt PII on removable storage media before mailing. Be sure to send passwords separately and always verify that the recipient received the information. Ensure any SPII, such as SSNs, are not visible on the outside or through the window of the envelope or package.

C. **Emailing SPII.**

a. **Emailing SPII within the Department.** SPII may be emailed to a recipient with an official need to know on the Department network because it is properly encrypted within the Department's network environment. Before emailing SPII within the Department's network, employees must confirm they have the correct email address and ensure the recipient is authorized to access and view the SPII. As a best practice to further mitigate the risks of a privacy breach, employees may choose to redact, password protect, or encrypt SPII when emailing within the Department's network.
b. **Emailing SPII outside the Department.** When emailing SPII outside the Department, employees must not put the SPII in the body of the email. Instead, they must create a password-protected attachment to the email and provide the password separately to the

recipient by phone or email. Employees must always confirm they have the correct email address and ensure the recipient is authorized to access and view the SPII.

c. **Emailing SPII to personal accounts.** Employees must not forward or send an email containing SPII to their personal email accounts unless it is encrypted and it's their own PII. Personal email accounts cannot be used to transmit or receive SPII for Government purposes.

Privacy Compliance Assessments

The Privacy Division participates in the cybersecurity program's annual Internal Control Review (ICR) to assess implementation control statements and verify they accurately describe how a system complies with NIST requirements. These assessments are completed in the Department's Governance, Risk & Compliance (GRC) tool.

Privacy Requirements for Websites and Social Media

Service employees must follow the Department's Website and Social Media Basics and other digital media guides when using social media and other sites.

A. **Link to privacy policy.** All Service websites, including those managed by contractors operating on behalf of the Service, must conform to current OMB guidance and Departmental requirements. A link to the Department, Service, or system-specific privacy policy, which includes the Department's children's privacy policy, must appear in the footer of every webpage regardless of whether information is collected from individuals.

B. **Social media.** Information (including PII) cannot be collected without authorization from the Service's Information Collection Clearance Officer (ICCO) and must not be collected directly through a social media platform.

Applying Privacy to Contracts

The Privacy Act applies to Federal contractors and partners who operate systems of records or handle Privacy Act-protected information. When we contract for the design, operation, maintenance, or use of systems containing information covered by the Privacy Act, contractors and partners are subject to the Federal requirements for safeguarding the information. Employees must ensure that contracts include appropriate Federal Acquisition Regulation (FAR) privacy and security contract clauses when the contractor has access to information relating to individuals. See the Department's Privacy Act regulations for contracts at 43 CFR 2.228 and the "IT Baseline Compliance Contract Guidelines" memorandum for more information.

Disposing of SPII

Employees must dispose of records containing SPII when no longer required consistent with the applicable records disposition schedules. If destruction is required, employees must take the following steps:

- Work with a Records and Information Management Specialist to complete FWS Form 3-2513, Regional/Program Records Disposition Certification.
- Shred paper containing SPII using an approved cross-cut shredder (NIST Special Publication 800-88, revision 1, Appendix A, Minimum Sanitization Recommendations). Do not recycle or place PII in garbage containers. The use of companies who supply secure shred bins is acceptable.
- Before transferring a computer or other device to another employee, or when a device is going to leave Service control, applicable digital storage media must be sanitized in accordance with IT Bulletin 2022-001, Digital Storage Media Sanitization Policy.

Remember to be especially alert during office moves and transitions when large numbers of records are at risk. Take steps to properly monitor and secure records and equipment at these times.

Privacy Act Requests and Disclosures

As mentioned previously in Chapter 2, employees must not disclose information from a system of records without consent of the individual or according to a routine use in a published SORN. There are some exceptions to the Privacy Act and some instances when you may disclose Privacy Act-protected information. Information may be shared when the disclosure fits within one of twelve specific exceptions to the Privacy Act that are in 5 U.S.C. 552a, which include exceptions for a need to know; Freedom of Information Act requests; statistical research purposes; and requests by law enforcement, Congress, and the National Archives. Prior to responding to any Privacy Act requests for records, employees should contact the APO or another member of the Service's privacy program for guidance by emailing FWS_Privacy@fws.gov. Responses to requests for records must be conducted in accordance with 43 CFR Part 2, Subpart K.

Certain information about Federal employees is also deemed public information and not ordinarily protected. Office of Personnel Management regulations direct agencies to release the following information about their employees: names, present and past position titles and occupational series, present and past grades, present and past annual salary rates (including performance awards/bonuses, incentive awards, etc.), present and past duty stations, and position descriptions. Consult 5 CFR 293.311 for more information.

Privacy Act System Managers must maintain an accurate record of every disclosure made from the system of records except with respect to public information, disclosures within the Department to employees in the performance of official duties, and disclosures to the individual. The record should identify the date of the disclosure, the person and agency to whom the disclosure was made, and the purpose of the disclosure. The record must be maintained for 5 years after it was made or the life of the record, whichever is longer. System Managers may use the DI-3710, Disclosure Accounting Form, for these purposes.

Chapter 4 - Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA)

PTA

PTAs are required as part of the Information Technology Purchase Approval (ITPA) process (for certain items) and IRTM's Requirements Management Board review for IMT projects. Program Managers, System Owners, and ISSOs must complete and submit a PTA to the APO for review and approval at the earliest stages of the information lifecycle. See the Privacy SharePoint site and the Department's PTA Guide for more information.

The purpose of completing the PTA is to:

- Identify programs, projects, information collections, and information systems that are privacy-sensitive, including certain non-IT projects like information collections or partnerships;
- Determine requirements for a PIA or adapted PIA or additional privacy compliance requirements for the maintenance, use, processing, sharing, or disposal of PII;
- Demonstrate that privacy considerations were included during the review of a program, project, etc.;

- Provide a record of the determination of privacy requirements for the System Owner and privacy program; and
- Demonstrate compliance with privacy laws, regulations, and policy.

PIA

PIAs are required for IT systems that maintain PII on members of the public. PIAs must be completed and approved by the Department's Senior Agency Official for Privacy to receive an authority to operate from the ACIO. Completing a PIA requires collaboration between the System Owner, Program Manager, ISSO, the Service Chief Records Officer, the APO, and the Departmental Privacy Officer (DPO) to ensure potential privacy risks are addressed and appropriate privacy protections are implemented. See the *IMT Project Review and Approval Handbook* for more information on how the PIA fits into the Service's project review and governance processes.

The PIA is an analysis of how information is handled, or specifically it is an assessment of how PII is maintained and disseminated. The PIA allows us to evaluate privacy risks, ensure the protection of privacy information, and consider privacy and security implications throughout the lifecycle of the system or application. PIAs must be updated with any significant change that affects the privacy posture of the system and are reapproved by the APO every 3 years. We may use a Departmentwide PIA if it accurately describes a Service system's information collection and practices; otherwise, a Service-specific PIA must be completed by the Program Manager, System Owner, and the ISSO in collaboration with the APO for approval by the DPO.

The APO will help to identify an existing PIA that covers the program, like O365, or work with the stakeholders to draft and finalize a new PIA. The PIA must be approved before the program may begin to collect PII. For further details, see the Department's PIA Guide or contact the APO for more information.

Chapter 5 - Privacy Breaches

A privacy breach occurs when we lose control of PII or it becomes compromised in some way, such as through unauthorized disclosure or acquisition. Some examples of scenarios where a privacy breach may occur include, but are not limited to:

- A laptop or portable storage device (e.g., external hard drive, flash drive, etc.) with stored PII is lost or stolen,
- An employee sends an email containing PII to the wrong individual,
- A box of documents with PII is lost or stolen during shipping,
- An unauthorized third party overhears Service employees discussing PII about an individual seeking employment or Federal benefits,
- An employee with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual,
- An information system that maintains PII is accessed by a malicious actor, or
- An employee posts PII that should not be widely disseminated on fws.gov or some other public website.

OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," requires Federal agencies to implement policy and procedures to respond to a breach of PII and includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach.

We follow the Department's Privacy Breach Response Plan in OMB M-17-12 for all suspected or confirmed breaches of PII in any medium or format.

A. **Reporting.** Employees must immediately report suspected or confirmed breaches of information about individuals to their supervisor, the IRTM Security Operations Center, the IRTM Enterprise Service Desk, or the APO per the instructions on the Privacy SharePoint site. The Department provides the Privacy Breach Reporting Form, DI-4009, that can be used for this purpose. Employees must NOT include the actual PII in the report as this would constitute another breach.

B. **Curiosity browsing.** Employees with access to SPII must only access it when there is an official need to know. Accessing records when there is no official need constitutes a breach and must be reported.

C. **Mitigating a breach.** The APO will provide guidance to mitigate the breach to the office or division responsible for the breach. The office or division responsible for the breach must fund any costs associated with mitigating the breach (e.g., notification letters to the affected individuals, credit monitoring, identity theft protection services). When appropriate, the APO will convene and lead the Service's Privacy Breach Response Team. The Privacy Breach Response Team works to investigate and mitigate reported breaches with other stakeholders such as the Security Incident Response Team, Human Resources Operations, Acquisition and Property Operations, and the DOI-Computer Incident Response Center.

D. **Credit monitoring and identity protection.** Employees must not offer affected parties credit monitoring and identity protection services without receiving approval from the Solicitor's Office.

Appendix A - Acronyms/Terms

Following are some common IT acronyms and terms that we use in this handbook.

Acronym	Description
ACIO	Associate Chief Information Officer
ACISO	Associate Chief Information Security Officer
APO	Associate Privacy Officer
CUI	Controlled Unclassified Information
DPO	Department of the Interior’s Privacy Officer
FISMA	Federal Information Security Modernization Act
FISSA	Federal Information Systems Security Awareness
GRC	Governance, Risk, and Compliance tool
ICR	Internal Control Review
IMT	Information Management & Technology
ITPA	Information Technology Purchase Approval process
IRTM	U.S. Fish & Wildlife Service Office of Information Resources and Technology Management
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Assessment
RBPT	Role-Based Privacy Training
Service	U.S. Fish & Wildlife Service
SORN	System of Records Notice
SP	Special Publication
SPII	Sensitive Personally Identifiable Information

Appendix B - Definitions

Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- An unauthorized user accesses or potentially accesses PII or SPII, or
- An authorized user accesses or potentially accesses PII or SPII for an unauthorized purpose.

Consent. An individual's permission to authorize the Federal Government to collect, use, maintain, or share their PII prior to its collection. Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy.

Disclosure. The release of information in a system of records to any person other than to whom the information pertains, including any employee of the Service, the Department, or employees of other Federal agencies. We must document disclosures on a DI-3710, Disclosure Accounting Form.

Information system. A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Maintain. The management, collection, use, or dissemination of records about individuals.

Member of the public. For the purposes of this chapter, any person who is not an employee of the Federal Government, including Tribal, State, and local government representatives when working in an official capacity. For example, a university biologist acting in their official capacity in partnership with the Service is a member of the public.

Personally Identifiable Information (PII). Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to an individual. Examples of PII include email addresses, phone numbers, photographs, license plate numbers, and logins or usernames. See the definition of sensitive PII below for more information.

Privacy Act System Manager (System Manager). Employee designated in the System of Records Notice (SORN) as having administrative responsibility for a system of records. The System Owner is usually also the Privacy Act System Manager.

Privacy Impact Assessment (PIA). An analysis of how information is handled to:

- Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of maintaining information in identifiable form in an information system; and
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy notice. A notice we give to individuals when they interact with a Service website, form, application, or system that collects PII. Privacy notices describe the authorities that allow us to collect PII, the reasons we are collecting it, our intended use for it (including sharing and dissemination), and any consequences of not providing the information. We often provide privacy notices in the form of Privacy Act statements.

Privacy Threshold Analysis (PTA). A tool used to identify privacy-sensitive projects, programs, and systems, and any potential gaps in privacy compliance, including the requirement to conduct a full PIA.

Record. Any item, collection, or grouping of information about an individual that the Service maintains (including, but not limited to, education history, financial transactions, medical history, criminal or employment history) that contains the individual's name or other identifier (e.g., fingerprint, photograph, etc.).

Routine use. An element of a System of Records Notice (SORN) that describes the purposes for which we are authorized to disclose a record.

Sensitive PII (SPII). A subset of PII that if lost, compromised, or inappropriately disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual or the Service. Examples of SPII are Social Security Numbers (SSN), credit card or financial account numbers, personal identification numbers, passwords, certain health or medical information, and employment records like negative performance appraisals or adverse actions.

System Owner. The employee or organization having responsibility for the development, procurement, integration, modification, operation, maintenance, and final disposition of an information system.

System of Records. A group of records under our control from which we retrieve information using an individual's name or other personal identifier. Systems of records are subject to the provisions of the Privacy Act.

System of Records Notice (SORN). A public notice in the *Federal Register* that describes a system of records. SORNs include:

- System name and number,
- Security classification,
- Name of the System Manager,
- Statutory authority for maintenance of the system,
- Purpose(s) of the system,
- Routine uses, and
- Additional items describing the system of records.