TABLE OF CONTENTS

1.1 What is the purpose of this chapter? This chapter establishes the responsibilities and procedures for the U.S. Fish and Wildlife Service's (Service) Privacy Act program.

1.2 What are the goals of the Privacy Act program? Our goals are to:

A. Protect the personal privacy of employees and the public when performing mission activities,

B. Ensure Service compliance with the Privacy Act when creating and maintaining systems that contain personally identifiable information, and

C. Reduce our risk related to Privacy Act matters.

1.3 What is the Privacy Act? Because the mission activities of Federal agencies sometimes require them to collect personal information about individuals, Congress wanted to protect individual privacy, so it passed the Privacy Act. The Act:

A. Applies to any paper or electronic system we use to collect and maintain personally identifiable information (PII). PII is information that directly identifies an individual (e.g., name, phone number, social security number, email address, fingerprints). PII may also consist of a combination of indirect data elements such as gender, race, birth date, geographic location (e.g., zip code), that we could use to identify specific individuals.

B. Establishes requirements for how Federal agencies must:

(1) Protect PII from unauthorized disclosure,

(2) Maintain and collect PII, and

(3) Set up procedures for allowing people to access and amend PII.

1.4 What are the authorities for the program?

A. Privacy Act of 1974 (5 U.S.C. 552a).

B. Children's Online Privacy Protection Act (COPPA) (15 U.S.C. 6501).

C. Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), (Public Law 104-106).

D. Computer Matching and Privacy Protection Act, revised 1990 (Public Law 100-503).

E. E-Government Act and the Federal Information Security Management Act of 2002 (Public Law 107-347).

F. Paperwork Reduction Act (44 U.S.C. 3501).

G. Presidential Records Act (44 U.S.C. 2201).

H. Freedom of Information Act (FOIA) (5 U.S.C. 552).

I. Equal Employment Opportunity Act (Public Law 92-261).

J. 383 DM 1 – 13, Public Access to Records.

K. Office of Management and Budget (OMB) Circular A-127, Financial Management Systems.

L. OMB Circular A-130, Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals.

M. Health Information Privacy Policy Act (HIPPA) Regulations (45 CFR 164).

N. Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR Part 2635).

O. Department of the Interior Regulations on Freedom of Information Act, Records and Testimony (43 CFR 2).

1.5 What terms do you need to know to understand this chapter?

A. Disclosure. Disclosure is when we disseminate or communicate (written, oral, electronic, or mechanical) information that we retrieved from a Privacy Act system of records.

B. Exempt system of records. In most cases, Federal agencies must allow people to directly access their records in systems of records (see section 1.5L) after we verify their identity. However, for some systems we do not have to allow access; these are "exempt systems of records." When addressing a Privacy Act request from an individual to access his/her records, it is important to know to what specific exemptions a system of records is subject.

C. Information collection. The Paperwork Reduction Act of 1995 (PRA) requires that Federal agencies obtain OMB approval before collecting most information from 10 or more persons. Under the PRA, "persons" includes individuals, corporations, universities, State/local/tribal governments, associations/organizations/partnerships, and foreign citizens/companies/governments. See the

information collection Web site and 281 FW 4 - 6 for more information about when OMB approval is required and the process for obtaining it.

D. Information system (IS). An information system is the infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

E. Matching agreement. A matching agreement establishes the terms of a matching program between two Federal agencies or a Federal and non-Federal agency.

F. Matching program. A matching program is a computerized comparison of two or more automated systems of records or a system of records with non-Federal records.

G. Privacy Act record. A Privacy Act record is any item, collection, or grouping of information about an individual that we maintain in a system of records (see section 1.5L), including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history. The record also must contain the name or identifying number, symbol, or other identifying item, such as a fingerprint, voiceprint, or photograph.

H. Privacy Act request. A Privacy Act request is an inquiry from an individual about the existence of, access to, or amendment of records about the individual (also known as access requests and first-party requests) that we keep in a system of records.

I. Privacy Act statement. A Privacy Act statement appears on a Web site, form, or other document and notifies users of:

(1) Our authority to collect requested information,

(2) The purpose and how we will use of the information,

(3) Whether providing the information is voluntary or mandatory, and

(4) Any right or benefit that we may deny the individual if he/she does not provide the information.

J. Privacy Impact Assessment (PIA). A PIA is an analysis of an information system to:

(1) Determine whether the system:

(a) Collects PII, and

(b) Conforms to applicable regulatory and policy requirements regarding the Privacy Act;

(2) Identify the risks of collecting, maintaining, and disseminating the information; and

(3) Examine and evaluate protections and alternative processes for handling information.

K. Record of access. A record of access is an accounting of when an individual or third party accesses an individual's record (excluding people whose job description requires them to routinely work with the Privacy Act records in question). The Privacy Act requires we keep records of access. Any requests for amendments to records and determinations about amendments should be in an individual's file. Electronic systems must be able to provide an audit trail of access and amendments.

L. System of records. A system of records is a group of any records under the control of an agency from which the agency stores and retrieves information using identifiers that are unique to the individuals in the system.

M. System of records notice (SORN). A SORN is a notice that an agency publishes in the Federal Register that describes the system of records under the agency's control.

1.6 Who is responsible for the Service's Privacy Act program? Table 1-1 lists the responsibilities of Service officials for the Privacy Act program.

Table 1 1: Privacy Act Program Responsibilities

These employees…	Are responsible for…
A. Director	**(1)** Providing for the general administration of the program and its effectiveness, and **(2)** Approving Privacy Act policy.
B. The Assistant Director – Information Resources and Technology Management	**(1)** Designating a Chief Privacy Act Officer, **(2)** Overseeing the Privacy Act program, **(3)** Ensuring staff in the Service comply with Privacy Act policies and procedures, and **(4)** Certifying completed corrective actions related to privacy as required by the Department.
C. Directorate members in Headquarters (HQ)	Ensuring staff within their programs comply with the Privacy Act policies and procedures.
D. Regional Directors	**(1)** Ensuring Regional staff comply with the Privacy Act policies and procedures, **(2)** Appointing a Regional Privacy Act Officer and an alternate and providing that information to the Service Privacy Act Officer, **(3)** Ensuring the Regional Privacy Act Officer: **(a)** Has adequate training and is knowledgeable about Privacy Act matters, and **(b)** Assist as needed in system design, development, or security.
E. Service Privacy Act Officer (PAO)	**(1)** Developing policy and procedures for the Service's Privacy Act program; **(2)** Maintaining and updating the privacy component of Departmental tracking systems; **(3)** Coordinating and providing advice and counsel to the Regional Privacy Act Officers and others involved in system development, design, and security; **(4)** Developing training regimens for programs and Regions as requested; **(5)** Serving as the privacy point of contact for the Bureau Incident Reporting Team; **(6)** Working with personnel officers to set policy on the appropriate risk/sensitivity level and screening requirements for positions with Privacy Act responsibilities; **(7)** Reviewing and assisting programs with PIAs, systems of records notices, narrative statements, and system design questions; **(8)** Coordinating with Contracting Officers and programs' representatives about contract and Memorandum of Agreement (MOA) requirements related to the Privacy Act; and

Table 1 1: Privacy Act Program Responsibilities	
These employees…	**Are responsible for…**
	(9) Leading the Bureau Identity Theft Task Force to resolve privacy breaches.
F. Regional Privacy Act Officers	**(1)** Developing Regional policy and procedures for the Service's Privacy Act program; **(2)** Maintaining and updating the privacy component of Departmental tracking systems; **(3)** Coordinating and providing advice and counsel to employees involved in system development, design, and security; **(4)** Developing training regimens as requested; **(5)** Serving as the Region's privacy point of contact for the Bureau Incident Reporting Team; **(6)** Working with personnel officers to set policy on the appropriate risk/sensitivity level and screening requirements for positions with Privacy Act responsibilities; **(7)** Reviewing and assisting employees with PIAs, systems of records notices, narrative statements, and system design questions; **(8)** Coordinating with Contracting Officers and programs' representatives about contract and MOA requirements related to the Privacy Act; and **(9)** Participating as needed in the Bureau Identity Theft Task Force to resolve privacy breaches.
G. DOI Learn Administrator(s) (appointed by the Director, National Conservation Training Center (NCTC))	**(1)** Coordinating with the Department to make Privacy Act training available through DOI Learn; **(2)** Maintaining and updating employee data in DOI Learn to ensure accurate information for the Service's Information Technology (IT) Security Manager to produce accurate reports; and **(3)** Assisting employees with technical issues related to accessing the Privacy Act training.
H. Chief Information Security Officer	**(1)** Working with the Service Privacy Act Officer on security issues that involve matters related to personal privacy; **(2)** Reviewing and signing PIAs as the Service's security representative; **(3)** Participating as a member of the Bureau Identity Theft Task Force; and **(4)** Assembling, leading, and organizing the Bureau Incident Reporting Team.
I. Managers/ Supervisors	**(1)** Ensuring that staff under their supervision who deal with Privacy Act systems or PII are knowledgeable of and adhere to the requirements of the Privacy Act, **(2)** Designating approved users to work with and be responsible for Privacy Act systems under their administrative control, and **(3)** Ensuring all employees under their supervision take required Privacy Act training.
J. Privacy System Owners	**(1)** Designating a Privacy System Manager for any Privacy Act system that is under their control or that they intend to create; **(2)** Ensuring that the Privacy System Manager is aware of his/her responsibilities, has adequate training, and has no ethical conflicts; **(3)** Overseeing the system of records for which they have administrative control; and **(4)** Coordinating with the Service Privacy Act Officer about establishing or modifying a Privacy Act system of records.

Table 1 1: Privacy Act Program Responsibilities	
These employees…	**Are responsible for…**
K. Privacy System Managers	**(1)** Preparing and reviewing PIAs for systems they manage or plan to manage; **(2)** Drafting systems of records notices, modifications, and narrative statements for systems they manage; **(3)** Coordinating with the Service Privacy Act Officer and their Regional Privacy Act Officer on Privacy Act complaints; **(4)** Ensuring that their Privacy Act records are timely, accurate, relevant, and complete; **(5)** Granting access and amendment requests to Privacy Act systems, as required; and **(6)** Maintaining records of access for Privacy Act systems and making the records of access available, as required.
L. Contracting Officers and Contracting Officers' Representatives	**(1)** Ensuring contractors who work with Privacy Act records or who handle PII are knowledgeable and trained about Privacy Act requirements, and **(2)** Ensuring that all contracts that involve Privacy Act systems of records have the requisite clauses and that contractors are held responsible.
M. Employees	**(1)** Adhering to Service Privacy Act policy and procedures, **(2)** Reporting violations of the Privacy Act or activities that might represent a Privacy Act breach to the Service's Privacy Act Officer and their supervisors, and **(3)** Taking required Privacy Act training.
N. Bureau Identity Theft Task Force	**(1)** Safeguarding PII collected, used, and maintained by the Service; **(2)** Providing advance planning, policy, breach incident coordination, and guidance regarding the actual and potential breaches of PII; **(3)** Meeting on an ad hoc basis to address incidents of breach; and **(4)** Requesting liaison services from the Interior Identity Theft Task Force as needed.

1.7 What are the elements of the Service's Privacy Act program? Exhibit 1 lists the elements of our Privacy Act program, how we perform activities for each element, and who is responsible for them. It covers, among other things, when to write a SORN to publish in the Federal Register, conducting PIAs, accessing Privacy Act systems of records, and the Privacy Act requirements for our Web sites.

1.8 What do employees have to do to protect PII?

A. Paper PII files: Employees must secure paper files that are in Privacy Act systems of records by keeping them in locked offices or locked file cabinets. The file cabinets must have Privacy Act warning labels. Employees must only use the files in secure locations (e.g., in employee offices and not in an airport or other public area) and file them away after using them.

B. Electronic PII files:

(1) *Employees must:*

(a) Password-protect the files,

(b) Encrypt the information before transmitting it,

(c) Not provide the information on public Web sites,

(d) When on travel, not leave laptops unattended,

(e) Carry laptops on board flights (do not check laptops in as luggage), and

(f) Only use the files in secure, limited access, low-traffic areas.

(2) *System managers must:*

(a) Limit access to the files to those who must access them, and

(b) Limit the ability to download PII.

C. OMB Directives: OMB directives related to the safeguarding and protection of PII can be found on their Web site.

D. Other Related Service Policy: IRTM also has security policy that addresses protecting PII information.

1.9 How must employees dispose of PII?

A. Paper PII files: Employees must destroy PII documents by shredding or burning them.

B. Electronic PII files: To destroy electronic files, employees must follow the guidelines at:

(1) IRM Bulletin 2001-004, Protecting Sensitive Data When Transferring, Donating, or Disposing of Computer Equipment;

(2) 383 DM 8, Safeguarding of Privacy Act Records; and

(3) 384 DM 1, Records Disposition.

1.10 What is a privacy breach and what happens if one occurs? A privacy breach occurs if an unauthorized person accesses, collects, uses, or discloses PII. The most common privacy breaches occur when personal information of customers, clients, or employees is lost, stolen, or mistakenly disclosed (e.g., lost or stolen laptops, transmitting PII to someone who does not have authorization to obtain the information).

A. All employees and contractors must report a suspected or evident breach immediately to the Service's Privacy Act Officer in IRTM. The employee/contractor should then report the breach to his/her supervisor.

B. The Service Privacy Act Officer will review the suspected or evident breach, analyze risk, and determine if he/she needs to report a breach to the Bureau Identity Theft Task Force. This team is comprised of the AD-IRTM; the Service Privacy Act Officer; and a representative from the Office of the Solicitor. If needed, the Service's Privacy Act Officer may add additional representation.

C. The Service follows OMB's breach and incident response guidelines, which are available on their Web site.

1.11 What are the civil remedies and criminal penalties associated with the willful or negligent handling of Privacy Act information?

A. People may bring a civil or criminal action against the Service related to Privacy Act information. Some situations that may trigger this action include if the Service:

(1) Determines that it will not amend a record at someone's request and the person disagrees;

(2) Fails to maintain a record about an individual as is necessary to ensure a fair determination related to the person's qualifications, character, rights, opportunities, or benefits; or

(3) Fails to comply with any requirement of the Privacy Act that affects the individual adversely.

B. If a court finds in favor of an individual filing a civil or criminal action, the court may:

(1) Order a correction,

(2) Order an amendment or release of records,

(3) Assign criminal penalties,

(4) Assess fines up to $5,000 dollars, and

(5) Require us to pay attorneys' fees and court costs.

1.12 What other documents are available that can help employees understand the Privacy Act and protecting PII? There are a number of documents related to the Privacy Act and protecting PII:

A. The Privacy Act of 1974 (Departmental Regulations).

B. System of Records Notices (Chapter 3, Document Drafting Handbook).

C. Narrative Statements (383 DM 5, Appendix 2).

D. Privacy Act Statements for:

(1) The Web.

(2) Contracts.

(3) File Cabinets.

/sgd/ Rowan W. Gould
DEPUTY DIRECTOR

Date: May 8, 2013