Elements of the Service's Privacy Act Program

What It Is	When We Do It	How We Do It
Privacy Act Impact Assessments (PIA)		
An analysis to identify: • Systems containing personally identifiable information (PII); • Risks to PII from collecting and maintaining the data; • When we may share PII with other departments or agencies; and • The physical security of the environment where the PII is processed/stored	We must conduct or update PIAs: • For every electronic system; • Before developing or procuring Information Technology (IT) systems or before collecting information electronically for 10 or more people; • When a system change creates a new privacy risk; • When information collection authorities, business processes, or other factors affecting PII change; and • At least every 3 years for existing systems that do not change.	System managers must conduct PIAs. They must use the Department's PIA template and route it for review and signature. The Service Privacy Act Officer must review PIAs and send them to the Assistant Director – Information Resources and Technology Management (AD–IRTM) for approval. • If the AD–IRTM clears a PIA, IRTM notifies the system manager and the system can be published on our Web site. • If the AD–IRTM does not clear a PIA, IRTM notifies the system manager and the system manager must modify the PIA accordingly.
System of Records Notice (SORN)		
A Federal Register notice with the following key components: • Systems name and number • System owner • System manager • Categories of records collected • Categories of individuals the records cover • Routine uses of the records • Information on how to access and amend the records • Safeguards, storage, and disposition requirements • Exemptions claimed for the system	We must publish SORNs when: • We create a new system of records (electronic or a collection of paper records) that maintains and generally retrieves information about an individual and contains information that describes the individual or presents a quality or characteristic unique to that individual; • We significantly change the system (e.g., change categories of users, categories of information, access or amendment procedures, exemptions); and • While conducting the PIA, the system manager determines that an existing system without a SORN has been modified and needs a full PIA.	System managers: • Prepare SORNs, • Coordinate with staff in the Division of Policy and Directives Management (PDM) to publish SORNs, and • Address public comments received on the SORNs The Service Privacy Act Officer assists programs preparing SORNs and reviews and approves SORNs before the system manager begins working with PDM.
Narrative Statement		
A summary of the SORN we use as a quick reference and put on our Web site.	We must prepare a narrative statement when we prepare the SORN.	The system managers or someone he/she designates prepares the narrative statement. System managers send the narrative statement to PDM with the SORN. PDM sends it to the Department and OMB with the SORN, but it is not

What It Is	When We Do It	How We Do It
		published in the Federal Register.
Privacy Act Reviews		
An analysis of Privacy Act systems to ensure compliance.	We must conduct these reviews biennially on all Privacy Act systems. Alternatively, a system manager may submit a 'self-assessment.'	The Service Privacy Act Officer: • Conducts the reviews, • Identifies deficiencies, and • Works with the system manager to determine corrective actions.
Federal Information Security Management Act (FISMA) Report		
A report on the security and Privacy Act aspects of the Service's electronic systems.	We report quarterly to Congress and OMB.	The Service's Privacy Act Officer and the Chief Information Security Officer coordinate to produce the FISMA report, which they draw from information in the Department's privacy and security tracking systems, personal knowledge of their program areas, and program submissions completed to comply with the Privacy Act, certification and accreditation exercises, and National Institute of Standards and Technology (NIST) standards. (Certification and accreditation is a process for implementing information security by evaluating, describing, testing, and authorizing systems before or after a system is in operation.)
Privacy Act Access and Amendment Requests, Tracking, and Reports		
People may request access to Privacy Act systems of records when those systems have information about them. We track the access requests. After accessing their records, people may request amendments.	Unless the system of records is exempt, we must allow access to citizens and lawfully admitted aliens to records: • About themselves when the request is in writing, unless the records are on-site and the requestor appears in person (e.g., to review his/her Official Personnel File (OPF)); • About themselves when the requestor provides proper identification (including photo identification and signature); • About someone else when the requestor shows written consent from the individual; and • About someone else when the requestor shows proof that he/she is the parent of a minor or the legal guardian of an individual who has been declared incompetent by a court. People may request access to records from the Service or	System managers process access requests. Regional Privacy Act Officers and system managers must report any disagreements about access to the Service Privacy Act Officer. If the Service Privacy Act Officer cannot resolve an access issue, he/she escalates it to the Office of the Solicitor. The Service Privacy Act Officer tracks and reports on access requests. After someone requests an amendment to a record, we must within 30 business days either make the correction or inform the person that we will not correct it and explain why. We must allow the person to file a statement explaining why he/she disagrees with us, and also notify the person of his/her right of judicial review of our decision. If the person files a statement of disagreement, the system manager must: • Clearly note any portion of the record he/she is disputing,

What It Is	When We Do It	How We Do It
	Regional Privacy Act Officer or the system manager.	• Provide copies of the statement of disagreement to the person, and • Work with the Service Privacy Act Officer to resolve the issue.
Privacy Act Complaints		
If a person witnesses or believes that the Service is not properly maintaining, disclosing, or disposing of records about him or her or someone else, the person may file a complaint with the Service Privacy Act Officer.	We accept written complaints addressed to: Service Privacy Act Officer Division of Information Resources and Technology Management Mailstop: 380 Arlington Square 4401 North Fairfax Drive Arlington, VA 22203 Complaints should include as much of the following information as possible: • Identifying information (photo identity/signature), • Information about what the issue of concern is and with what records (if known), and • Names of people involved in the perceived violation, and dates (if known).	The Service Privacy Act Officer works to resolve the complaint. If he/she cannot resolve the complaint, then the matter is referred to the Office of the Solicitor. The Privacy Act Officer must keep the complaint for 6 years from the date it's filed.
Awareness and Training		
The National Conservation Training Center (NCTC) provides required training on Privacy Act information and issues for all employees and contractors.	Employees and contractors who access Service IT systems must take Privacy Act training annually through the DOI Learn online system.	If employees and contractors do not take required training, we may suspend their access to Privacy Act–protected information. NCTC tracks completion of training. Employees and contractors must also: • Read and sign the rules of behavior, and • Make sure their user names and passwords are current. When requested, the Service and Regional Privacy Act Officers may provide additional training and consultation. Each year the Privacy Act training is delivered as part of the "Federal

What It Is	When We Do It	How We Do It
		Information Systems Security Awareness + Privacy and Records Management (FISSA+)" course. This training is automatically assigned to all Employees and Contractors and appears in the "My Learning" section in the right column of the DOI Learn home page. It can also be accessed under the "Access My Required Training" icon, also found on the home page. Log in to DOI Learn at: www.doi.gov/doilearn/index.cfm Each year the Service IT Security Manager prepares completion reports drawn from DOI Learn and distributes them to the appropriate officials. Regional Security Managers will work with offices to ensure that all Service employees and contractors have the opportunity to complete the training. Those subject to the annual requirement who fail to complete the FISSA+ training are at risk of having their access to Service networks revoked until the requirement has been met.
System Design and Review		
By asking the Service Privacy Act Officer to review system design, programs can save time and effort for reporting on compliance with the Privacy Act.	When a program is planning the creation of a system of records or making a significant change to an existing system.	The Service Privacy Act Officer must assist programs, upon request, to determine designs for systems that will reduce PII and safeguard privacy.
Public Web Sites and Privacy Policies		
Our public Web sites must comply with privacy laws and OMB privacy-related memoranda by including a notice about the nature, purpose, use, and sharing of information on our sites.	For all public Web sites.	Web site system managers must ensure their sites: • Prominently display a Privacy Act statement, • Inform visitors to the site about how we grant consent for the use of information they provide on the site, • Inform visitors about their rights under the Privacy Act, • Inform visitors if collected information is maintained or retrieved by personal identifier, • Inform visitors about what information we may gather automatically (e.g., user IP address, location, time of visit), and why (e.g., site management, security), • Use tracking technology such as 'persistent cookies' only when the Director approves it and report the use of persistent cookies to OMB, • Use clear language to describe our practices of protecting information to prevent attacks on the site's information and systems,

What It Is	When We Do It	How We Do It
		• Incorporate requirements of the Children's Online Privacy Protection Act for sites that provide content to children under the age of 13, • Where applicable, indicate the sharing of collected information for authorized law enforcement purposes, and • Provide technical mechanisms to translate privacy policy into a standardized machine-readable format.
Computer Matching Activities		
We may compare a Privacy Act system with another system to produce a match (e.g., benefits and parents not paying child support)	When the comparison: • Supports mission activities, and • After a Data Integrity Board reviews and approves a written agreement between the source agency and the recipient agency.	We must work with the non-Service agency to develop a written agreement about the matching activities. The Department establishes the Data Integrity Board. The Integrity Board must review and approve written agreements before the comparison takes place. The Board also maintains the agreements. The recipient agency maintains the results of the comparison.