United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240

SEP 2 1 2007

TAKE PRIDE IN AMERICA

OCIO Directive 2007- 005

To: Deputy Secretary
Assistant Secretaries
Deputy Assistant Secretaries
Deputy Associate Secretary
Heads of Bureaus and Offices
Bureau Chief Information Officers

From: Michael J. Howell
Chief Information Officer and
Senior Agency Official for Privacy

Michael Howell

Subject: Departmental Strategy to Safeguard Personally Identifiable Information and Reduce the Collection and Uses of Social Security Numbers

Purpose:

Recent direction from the Office of Management and Budget (OMB) (OMB Memorandum M-07-16), Office of Personnel Management (OPM) memorandum dated June 18, 2007, and the Federal Identity (ID) Theft Task Force (July 2007 white paper) provide Government offices maintaining information on individuals with new requirements for minimizing the use of personally identifiable information (PII)[1] in paper, electronic, and all other formats, safeguarding such information, and addressing incidents involving potential breaches of PII. Some of these requirements will be evaluated in future Federal Information Security Management Act (FISMA) and Inspector General reviews. Future updates to this document will be provided when necessary. The Department of the Interior's (DOI) "privacy protection strategy" to implement these new guidelines is summed up below and the bureau/office actions that need to be taken will be explained in Attachment I of this document:

1. Discover the PII your organization maintains;
2. Reduce use of PII and Social Security Numbers (SSNs);
3. Replace SSNs with an alternative identifier; and
4. Protect PII and address potential incidents of breach.

Privacy protection measures will require the collaboration of all employees and especially those involved with making decisions on collecting information, developing systems that maintain PII,

[1] Refer to the definition of PII in OMB Memorandum M-07-16 at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf. ("Personally identifiable information" is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as a date and place of birth, mother's maiden name, etc.")

owning and maintaining these systems, safeguarding the information, reporting incidents according to US-CERT requirements, making decisions on the use and disclosure of the information, and managing reporting tools that address the Government privacy protection requirements.

The Office of the Chief Information Officer (OCIO) has evaluated these new guidelines (see Attachment II), and incorporated them into this Departmental privacy protection strategy. This Directive covers the new privacy requirements that affect DOI and bureau privacy programs. Those requirements affecting Cyber Security, the DOI ID Theft Task Force (ITTF) "Privacy Loss Mitigation Strategy" (PLMS) (following-up on breach incidents and notifying persons affected), and National Institute of Standards and Technology (NIST) requirements will be highlighted in separate guidance documents.

This document provides action items that bureau/office Chief Information Officers (CIO) must ensure are completed for offices in their oversight by the specified dates. One major action requires immediate attention that CIOs direct the establishment of an on-going bureau/office Information Reduction Team (IRT) to address the reduction of PII and SSN collection and use. Goals these Teams must achieve are addressed in Attachment V. Teams will require the collaboration of program leads (who request PII and SSN collections), Information Collection Clearance Officers, Data Architects, IT Security Program Managers, legal counsel, and Privacy Officers.

Background:

The E-Government Act of 2002, recent OMB guidelines on safeguarding PII, and Government requirements for dealing with incidents in addition to existing Privacy Act requirements for maintenance of information on individuals (see Attachment II), support the Government and Department's proper management of PII. The Department is dedicated to meeting a level of excellence as stewards of the information entrusted to the Department as expressed in the Secretary of the Interior's memorandum of June 2006.

Safeguarding personally identifiable information in the possession of the Government and preventing its breach are essential to ensure that Government retains the trust of the Department's customers.

Actions:

(See Attachment I)

Scope:

The Department's privacy protection strategy applies to all persons within the Office of the Secretary and those involved with decisions on collecting information, developing systems that maintain PII, owning and maintaining these collections or systems, safeguarding the information, reporting incidents according to US-CERT requirements, making decisions on the use and disclosure of the information on behalf of the DOI, and managing reporting tools that address the Government privacy protection requirements.

Due Dates:

Each bureau and office must set up Bureau/office Information Reduction Teams to address the reduction and replacement of PII and SSNs by October 12, 2007. Action items must be completed by the dates specified in Attachment I.

Contact:

For questions concerning this memorandum contact the Departmental Privacy Office at (202) 208-6194, Information Management Division, Office of the Chief Information Officer, MS 5312 MIB.

Attachments:

I. Action Items for the DOI Privacy Protection Strategy
II. Recent Guidelines on Collecting and Safeguarding PII and Reducing the
III. Collection and Use of SSNs
IV. Privacy Fields Form for the DEAR
V. Business Process Privacy Fields Form for the DEAR
Information Reduction Team Goals
VII. Checklist for Privacy Record Maintenance Requirements
VIII. Sample E-FOIA Tracking System Rules of Behavior

cc: Bureau/Office Privacy Officers
Information Collection Clearance Officers
Bureau Information Technology Security Managers
Data Architects

Attachment I

DOI Privacy Protection Strategy

I. Discovery

The Principle: Know where Personally Identifiable Information (PII)[2] and Social Security Number (SSN) information are maintained at all levels of your organization to ensure that proper safeguards are in place. This will also assist in incident reporting.

A. Action Needed:

1. PII and SSNs in DEAR: Privacy fields were added to the Departmental Enterprise Architecture Repository (DEAR) in December 2006 to identify which systems maintain PII and SSNs and other privacy characteristics pursuant to privacy requirements. These privacy fields must be populated as soon as possible. It is imperative that those responsible for maintaining the **Accreditation Boundary and System list and System Inventory records** in DEAR update the privacy fields.

Due Date: Please ensure that these fields (identified in Attachment III) are completed in DEAR and verified with the Bureau/Office Privacy Officer (or alternate selected by the organization) who will coordinate the input into DEAR by December 31, 2007.

2. Business Processes and PII and SSNs: In December 2006, OMB required all federal agencies to review their use of Social Security Numbers (SSNs) to determine whether such use can be eliminated, restricted, or concealed in agency business processes, systems and electronic forms. According to OMB instructions for the survey, "Process Name" means: "Provide the name of the business process, system, or paper/electronic form, other than those authorized by OMB, which use, collect or receive an individual's SSN or truncated SSN. Include major processes of the agency's mission as well as processes that are common to all agencies (i.e. payroll, research and quality)". Since then OMB has extended the same analysis to the collection and use of PII.

In order to track these business processes, DEAR was enhanced August 2007 to identify whether business processes collect and use PII and SSNs. For those business processes that were not identified in the December 2006 survey to OMB (e.g., new processes that collect SSNs and those that collect PII), please have program leads complete Attachment IV and provide this to your Privacy Officer (or alternate selected by the organization) who will coordinate input into DEAR.

---

[2] *Id* at 1.

Due Date: This process should begin immediately and be ongoing as new business processes are developed that collect PII and SSNs.

3. Reduce PII by Updating and Publishing Privacy Act System of Records Notices (SORN)

OMB Memorandum M-07-16 (Attachment 1.A.) states that: "The Privacy Act also requires personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete including through the use of notices to the public. It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and OMB's implementation policies. By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it."

Ensure that your organization's SORNs are updated and accurate, and that a SORN is published for new system of records. OMB Circular A-130, Appendix I states that "agencies are also required to publish notice of any **subsequent substantive revisions to the use of information** maintained in the system of records."

The OMB Memorandum M-07-16 (Attachment 2, B. 2) also requires that new "routine use" disclosures be included for those systems of records where information may need to be shared to coordinate investigations of breaches.

Due Date: By December 31, 2007, provide to the DOI Privacy Office the list of systems of records from your bureau/office that requires a new SORN, existing SORNs for which there are subsequent use revisions and a revised notice is required, and systems of records requiring the "routine use" language provided in the OMB memorandum. System Managers for new systems of records should publish a new SORN immediately if they have not done so already.

II. Reduce Collection and Use of PII And SSNs

The Principle: Only collect information that is absolutely necessary to perform an agency function and that is authorized.

A. Action Needed:

1. Bureau Information Reduction Teams:

Background: The OMB Memorandum, M-07-16, Attachment I, Section B (pg. 6), requires that agencies must now review their current holding of all personally identifiable information and ensure such holdings are accurate, relevant, timely and

complete, and reduce them to the minimum necessary for proper performance of a documented agency function. (The inventories above under Section I include business processes that will help identify the collections of PII and SSNs.)

The memorandum also indicates that agencies must also review their use of SSNs in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of the memorandum (dated May 22, 2007), agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of SSNs within eighteen months. DOI will meet this requirement by implementing this Directive. Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual report under FISMA. Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings.

Bureau requirements: The Chief Information Officer for each bureau/office is required to oversee the organization of **Information Reduction Teams** in their bureau/offices that will meet certain standard Department-wide goals identified in Attachment V.

Due Date: Bureau/Office Information Reduction Teams must be established by October 12, 2007 to begin plans to eliminate unnecessary collection and use of SSNs within eighteen months (by March 2008).

Each Team will create a plan that will identify those collections of PII and SSNs collected by their organization, the timeline when program offices will review the necessity for the collection, and the timeline to make changes to eliminate the PII or SSN found to be unnecessary or provide an alternative. Provide a copy of the list and plan to the Departmental Privacy Office by December 28, 2007,

Those identified should be eliminated or replaced by November 2009. According to the OMB Memo M-07-16, agencies must develop and make public a schedule by which they will periodically update the review of their holdings (See Attachment 1(B)(1)). **The Office of the CIO will require updates from each bureau/office Team coinciding with FISMA Quarterly reporting schedules.**

Note: In cases where alternate identifiers for SSNs may need to be examined at the Department level because of the impact changes may have to other Departmental systems, the bureau/office Information Reduction Teams may request that the Departmental CIO designate a team involving expertise from Data Architects and Chief Technology Officers to assist them in addressing the issues.

III. Protecting PII And SSNs

The Principle: Ensure all Government agencies take appropriate measures to safeguard and protect PII.

A. Action Needed

1. OCIO Directive 2006-16, Attachment III: "Checklist on Maintaining Privacy Act Information". Bureaus were provided with a checklist in June of 2006 to ensure that appropriate safeguard measures were in place when maintaining information on individuals. See Attachment VI below for a copy of that checklist. Bureaus/offices must ensure that wherever PII is maintained in the organization, appropriate safeguards are in place and employees understand the limitation of disclosure and use of that information.

2. Complete Privacy Impact Assessments (PIA) for PII Systems. PIAs address safeguard, collection, use and other maintenance requirements and provide a Privacy risk assessments for systems as they are designed, developed, maintained and modified. Ensure that PIAs are completed throughout the system development life cycle. See Safeguarding Privacy Act Records: DOI Manual Section 383 DM 8; and DOI Privacy Act regulations at 43 CFR 2.51 (b) at http://www.doi.gov/foia/43cfrsub.html.

3. Mandatory Privacy Act Computer-based Training: Ensure that all personnel involved in the handling of agency records undergo annual training. The OCIO has developed mandatory computer-based training (CBT) for all persons handling PII entitled "Privacy Act Orientation." This is available on DOI Learn.

4. Understanding of Responsibilities: The Office of Management and Budget Memorandum,
M-07-16 (Attachment 1, C. (pg.8)) states that: "Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities." This will help to ensure that any additional guidance on the special handling of information from that system will be understood.

As a means for the Department to implement this requirement all such employees with access to PII and their supervisors must sign at least annually a document such as that provided in Attachment VII.

5. DOI Privacy Act Regulations on the Maintenance of Privacy Act Records: Ensure that the minimum safeguard requirements in the DOI regulations are explained to all personnel who handle or have access to Departmental PII information. See 43 CFR 2.48 at http://www.doi.gov/foia/43cfrsub.html and Departmental Privacy Act Manual Section 383 DM 8 (includes Illustration I, "Privacy Act Warning Notice") at http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3454.

6. Privacy Act Code of Conduct for DOI Employees: Ensure that personnel that handle or who have access to Departmental PII information are aware of these regulatory requirements. See 43 CFR 2.52 at http://www.doi.gov/foia/43cfrsub.html.

7. Office of Personnel Management (OPM) Guidelines on Protecting Personnel Information and SSNs: Personnel making decisions on personnel information and their safeguarding must be familiar with guidance in the Departmental Manual Section 383 DM 6, Appendix I (http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3452).

Such personnel must also have knowledge of the OPM Memorandum for Chief Human Capital Officers dated June 18, 2007 on "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft" (http://www.chcoc.gov/transmittal_detail.cfm?ID=847).

Attachment II

Recent Guidelines on Collecting and Safeguarding Personally Identifiable Information (PII)[3] and Reducing the Collection and Use of Social Security Numbers

1. OMB Paper on "Common Risks Impeding the Adequate Protection of Government Information" dated July 2007 (http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf).

2. Office of Personnel Management memorandum on "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft" dated June 18, 2007 (http://www.chcoc.gov/transmittal_detail.cfm?ID=847).

3. OMB Memorandum M-07-16 on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" dated May 22, 2007 (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf).

4. OMB Memorandum on "Recommendation for Identity Theft Data Breaches Which Could Result in Identity Theft" dated September 20, 2006 (http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

5. OMB Memorandum M-06-19 on "Reporting Incidents Involving Personally Identifiable Information" dated July 12, 2006 (http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf).

6. OMB Memorandum M-06-16 on "Protection of Sensitive Agency Information" dated June 23, 2006 (See http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf - listing security requirements agencies must implement such as encryption, control remote access, time-out functions, log and verify features, and notification of responsibilities for personnel that handle PII and SSNs).

7. OMB Memorandum M-06-15 on "Safeguarding Personally Identifiable Information" dated May 22, 2006 (http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf).

8. OMB Memorandum M-03-22 on "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" dated September 26, 2003. (Implementing Privacy Impact Assessments and Web privacy requirements, http://www.whitehouse.gov/omb/memoranda/m03-22.html).

---

[3] According to OMB Memorandum M-07-16, PII is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Previous Departmental Guidelines on Safeguarding Information on Individuals

1. OCIO Directive 2006-16 on Safeguarding PII of June 2006. See Attachment III "Checklist on Maintaining Privacy Act Information" at http://www.doi.gov/ocio/privacy/Interior%20Privacy_Assessment_Template_No%20Explanations.doc.

2. Safeguarding Privacy Act Records: DOI Privacy Act regulations at 43 CFR 2.51 (b) (http://www.doi.gov/foia/43cfrsub.html).

3. Standards for Maintenance of Privacy Act Records: 43 CFR 2.48 (http://www.doi.gov/foia/43cfrsub.html).

4. Code of Conduct for Employees: 43 CFR 2.52 (http://www.doi.gov/foia/43cfrsub.html).

5. Safeguarding Privacy Act Records : DOI Manual Section, 383 DM 8 (Also note the Privacy Act Warning Notice of Illustration I) (http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3454).

6. Making decisions on Personnel Information (includes OPM memo guidance): See 383 DM 6, Appendix I at http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3452.

7. OMB Memorandum M-03-22 on "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" dated September 26, 2003. Review sections on Privacy Impact Assessments for Paperwork Reduction Act information collection packages. (http://www.whitehouse.gov/omb/memoranda/m03-22.html).

Previous Departmental Privacy Guidance on Information Collection

1. DOI Privacy Impact Assessment, Section D examines the authority and reason for the collection of the data for the system (http://www.doi.gov/ocio/privacy/Interior%20Privacy_Assessment_Template_No%20Explanations.doc).

2. The Privacy Act system of record narrative statements discuss the authority and minimization of information needed. See 383 DM 5, Appendix II (http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3451).

3. Making decisions on collecting information (includes the minimization principle) and the Privacy Act notification required on forms. See 383 DM 4.7 (http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum= 3450).

4. Social Security Number Use: 383 DM 11 (http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3457).

Attachment III

Privacy Fields for DEAR	**Date:**	
Name of System:	C&A Boundary? (Yes__No__) System?(Yes__ No__)	
A. For "Contact Tab"		
Owner: Name: Office:	Phone Number:	Email:
System Manager (Responsible for ensuring that the legal requirements for the system are in place): Name: Office:	Phone Number:	Email:
PIA Contact (Responsible for ensuring the PIA is completed and signed): Name: Office:	Phone Number:	Email:
B. For "Privacy Tab"		
1. When was a preliminary Privacy Impact Assessment (PIA) completed? (Preliminary PIA are required on all systems to determine if there is information on individuals maintained in the system)	Date:	
2. Does the system contain any Federally-owned information about individuals?	No____**(If "No" no further information required)** Yes___ **(If "Yes" complete the questions below)**	
	a) Is the information identifiable to the individual? (Can be linked back to the individual using a unique identifier?)	Yes____ No____
	b.) Is the information about individual members of the public? (Right now the OMB FISMA report and Exhibit 300s just require reporting on these systems)	Yes____ No____

	c.) Is the information about employees? (DOI's policy is to require PIAs for systems with this information. The C&A also requires PIAs for these systems and those in "b)" above)	Yes____ No____
	d) Does the system contain information on individuals doing business with the Government? (Individual entrepreneur who may be working out of their home for example)	Yes____ No____
3. Privacy Impact Assessment Required? (A full PIA is needed because the system contains information identifiable to the individual)	Yes ____ No____	Completion Date:
4. Is Federally-owned information retrieved by name or unique identifier? (Will help to identify Privacy Act system of records that require system notices (SORN))	Yes ____ **(If yes proceed to questions below)** No ____ N/A___	
	a) Does the system contain a Privacy Act System of Records Notice (SORN)? (List the SORN -- e.g., BIA-4: Indian Land Records: or if more than one SORN covers it, list them)	SORN:
	b) Was an online form used to collect the Privacy Information? (E.g., interactive form that collects information from a website and is fed into a database)	Yes ____ (Go to questions (1) and (2) below) No ____
		(1) OMB approved Form(s) number(s)_____

		(2) Does the web page housing the form have the appropriate web privacy notices? (An E-Gov requirement reported to OMB) Yes____ No____
5. Does the system maintain SSNs? (OMB asks this when there is a breach to a system)	Yes ____ No ____	
6. Does the system maintain financial information? (OMB asks this when there is a breach to a system)	Yes ____ No ____	
7. Does the system maintain health information? (OMB asks this when there is a breach to a system)	Yes ____ No ____	
8. How many individuals have identifiable information in the system? (OMB asks how many individuals may be affected by a breach to a system)	Number _____	

Name and Signature of Bureau/Office Official Authorizing that the Information Can be Inputted into DEAR	Name:_____ Contact Information:_____	Signature:_____

Refer to the definition of PII in OMB Memorandum M-07-16 at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf. ("Personally identifiable information" is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as a date and place of birth, mother's maiden name, etc.)

Attachment IV

Processes[1] that Collect and Use PII and SSNs									
Process Name	**Internal / External Interagency**	**Mission Related / Administrative**	**Is PII Collected (yes/no)?**	**Authority for the Collection (legal authority to collect PII)**	**Function Served by PII**	**Are SSNs Collected (yes/no)?**	**Authority for the Collection (legal authority to collect SSN)**	**Function Served by SSN**	**Contact for the Collection (name, Office, phone number and email)**

Name and Signature of Bureau/Office Official Authorizing that the Information Can be Inputted into DEAR	Name:_____ Contact Information:_____	Signature:_____

[1] . According to OMB instructions for the survey, "Process Name" means: "Provide the name of the business process, system, or paper/electronic form, other than those authorized by OMB, which use, collect or receive an individual's SSN or truncated SSN. Include major processes of the agency's mission as well as processes that are common to all agencies (i.e. payroll, research and quality)"

Attachment V

Information Reduction Team Goals

Bureau/Office Information Reduction Teams must be established by October 12, 2007

I. Information Reduction Team member make-up:

- CIOs will identify the bureau/office leaders for the Team.
- Information Collection Clearance Officer
- Data Architect
- Privacy Officer
- IT Security Manager or BITSM
- Representative from program areas for which information is collected, used and examined.
- When necessary, the program attorney from the Solicitor's Office familiar with the need to collect the information will be consulted.

II. Each Team will create a plan that will identify those collections of PII and SSNs collected by their organization, the timeline when program offices will review the necessity for the collection, and the timeline to make changes to eliminate the PII or SSN found to be unnecessary or provide an alternative. Provide a copy of the list and plan to the Departmental Privacy Office by December 28, 2007.

Those identified should be eliminated or replaced by November 2009 (within 18 months of the OMB Memorandum as required by OMB).

III. According to the OMB Memo M-07-16, agencies must develop and make public a schedule by which they will periodically update the review of their holdings (See Attachment 1(B)(1)). **The Office of the CIO will require updates from each bureau/office Team coinciding with FISMA Quarterly reporting schedules.**

IV. Examine the inventory of processes and collections of PII and SSNs for which each bureau/office is responsible and identify program leads responsible for those collections. The processes and collections of PII and SSN were examined by bureaus in December 2006 for the OMB survey. DEAR is also enhanced to include these new privacy fields which bureaus must populate.

V. Review the legal authority for collecting that information and alternatives for the collection and use of that information in information systems and business processes.

VI. Conduct a preliminary assessment of collections with PII and SSNs. Identify which ones are a high priority (based on risk, impact and cost) for the follow up review. Then, develop a plan to redact, retire, eliminate or maintain that information/collection as needed.

VII. Track uncorrectable systems of unnecessary and/or unused SSNs and PII. Consider the early retirement or replacement of these systems.

VIII. Uncorrectable systems tracked via Plan of Action and Milestones (POA&M).

IX. For systems that must maintain the collection of PII and SSNs, develop methods to increase protection of that information (masking, reducing access, etc.). Suggestions below:

i. Use an internal person number, instead of social security numbers, to link database records.

ii. Generate an Employee Common Identifier (ECI), a number that is used to uniquely identify an employee for each Agency/Department. This number should be used, instead of social security numbers, for reporting purposes and internal Departmental/Agency subsystems. **Note**: All bureaus and offices should contact the Department's Enterprise Architect, prior to developing their own unique ECI solutions, in order to take advantage of any Departmental ECI solutions available at that time.

iii. Mask or redact the social security numbers on any reports or records that are sent to external entities.

X. Ensure existing policy on limiting collection of information is implemented in offices:

i. DOI Privacy Impact Assessment Section D details the collection criteria of data for the system at http://www.doi.gov/ocio/privacy/Interior%20Privacy_Assessment_Template_No%20Explanations.doc.

ii. The Privacy Act system of record narrative statements which are sent to OMB and Congress with system of records notices discuss the authority and minimization of information needed. See 383 DM 5, Appendix II at http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3451.

iii. Making decisions on collecting information (includes the minimization principle; only collect what is actually needed and for which you have a legal authority to collect): 383 DM 4.7 at http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3450.

iv. Comply with DOI Manual Section 383 DM 11 on Use of SSN http://elips.doi.gov/app_DM/act_getfiles.cfm?relnum=3457.

XI. Identify a Records Management Representative to conduct on-site visits to regional offices for compliance reviews with all applicable record keeping requirements. Findings should be documented in a report and submitted to the Chief Appraiser and to the Senior Records Management Officer.

Attachment VI

Checklist for Privacy Records Maintenance Requirements

The attached checklist is based on:

- Privacy Act guidance found in the Department of the Interior (DOI) Privacy Act Manual Section (383 DM Chapters 1 – 13)
- DOI Privacy Act regulations at 43 CFR 2.45 – 2.79
- OMB Circular A-130, Appendix I
- E-Government Act of 2002
- Personnel Bulletin No. 05-02 issued February 18, 2005 on Departmental Telework Policy.
- Federal Information Security Management Act (FISMA)
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard Publications (FIPS Pubs) and Special Publications (SP)
- 375 DM 19 (All IT security and C&A roles and responsibilities are specified in the Departmental Manual (DM 375 Chapter19). The C&A roles and responsibilities are further elaborated on in each of the applicable NIST standards)

On-Site Inspection for Privacy Records Maintenance Requirements

Date:_____ Name of System: _____

Name of Privacy Act System of Records Notice that Covers the System: _____

If a Privacy Act system of records is required, date that one will be prepared _____

System Manager for System_____ Bureau/Office Privacy Officer/Coordinator _____

Bureau/Office Information Technology Security Manager_____

Requirement and Guidance Cite	Compliant (Yes/No)
I. Physical Security of the Area	
a. Do the manual record systems comply with the DOI Privacy Act regulatory safeguard requirements at 43 CFR 2.51?	
b. Is a Privacy Act "Warning Notice" posted in records system areas that are not automated? **383 DM 8.3 and Illustration I. and 43 CFR 2.51(b)**	
c. If this is an automated system, is a Privacy Act Warning Notice or equivalent made available to those who have access to the Privacy Act system of records (e.g., JAVA scripted pop-up notice)?	

Requirement and Guidance Cite	Compliant (Yes/No)
d. If this is an automated system, is there documentation that ensures that 383 DM 8.4 and 43 CFR2.51 are implemented?	
e. If this is a computerized system, does the IT System Security Plan (SSP) appropriately identify that this is a Privacy Act system of records?	
f. Are these records covered by an Office of Personnel Management (OPM) Central Privacy Act system of records notice? (e.g., employee clearance files). Is it clear that OPM must be contacted regarding decisions on the information.	
g. If these are OPM managed files, do they meet the security requirements set out by OPM regulations 293.106 and 293.107 (See 5 CFR 293)? **43 CFR 2.51(d) & 383 DM 8.6**	
h. Are paper records properly secured and not made visible to those who do not have a "need to know" the information?	
i. Are computer terminals which may display sensitive information properly placed in order that only those who have a "need to know" can view the information?	
j. If there are no locked cabinets, do doors to the rooms have locks to ensure that only those who have a "need to know" will have access?	
II. Instructions to Employees Handling the Information	
a. Is there a Privacy Act system of records published and available for persons making decisions on the information system?	
b. Are system guidelines in place for employees working with a system of records? For example are there operating procedures to be followed in maintaining a specific records system and supplement the DOI regulations **(383 DM 1.4.G., 43 CFR 2.51(c))?**	
c. Are system managers familiar with the Privacy Act disclosure and use restrictions for this grouping of information **(43 CFR 2.56)?**	
d. Do the IT Security business rules address the specific handling and disclosure and "need to know" access restrictions identified in the Federal Register notice for this system **(OMB A-11 (See Exhibit 300 "Security/Privacy" section))?** **[Individuals with access to PII and their supervisors must sign at least annually a document (e.g., EFTS Rules of Behavior, Attachment VII) clearly describing their responsibilities. (See OMB Memo M-07-16, Attachment I, C., Pg. 8).]**	
e. Are employees who manage, use, or handle information from the Privacy Act system familiar with the Privacy Act and regulatory requirements and familiar with any special requirements that their specific jobs entail? **383 DM 3, Appendix I** **43 CFR 2.52: Conduct of Employees** **43 CFR 2.51(c)** **383 DM 3.11** **383 DM 7: Disclosure Procedures** **383 DM 8: Safeguarding** **383 DM 9: Handling PA Records**	
f. Was a Privacy Impact Assessment done for the automated system?	
g. Was it used to help identify the privacy concerns and handling requirements?	

Requirement and Guidance Cite	Compliant (Yes/No)
h. Do contractors manage, use or handle information from the Privacy Act system? 1. Do contracts have appropriate Federal Acquisition Regulation (FAR) and DOI Acquisition Regulation privacy clauses (see FAR 52.224-1and Privacy Act Notification at FAR 24.104(a), supplemental information at DIAR 1452.224-1, and 43 CFR 2.53)? 2. Have contractors responsible for DOI information on individuals taken appropriate Cyber Security, Privacy and Records Management training?	
i. If yes to the above, are contractors provided with Privacy Act and DOI guidelines on handling the Privacy Act information, and with the specific instructions for this particular system? (e.g., business rules, *Federal Register* notice)	
j. Ensure that bureau/office telework policy is implemented and consideration is made regarding the appropriateness of using information on individuals and agreements are signed (Personnel Bulletin No. 05-02 issued February 18, 2005. Especially sections 3.1.Q. on "Security and Liability Issues"; 3.1.S. on "Privacy Act Considerations"; 3.1. U. on "Recordkeeping Requirements"; and compliance with items on records, privacy and security in the telework agreement.)	
III. Accounting for Disclosures	
a. The Privacy Act requires that records be kept on all disclosures and made under the exceptions described in 2.56(c). Is there an accounting log or accounting system in place to track disclosure requests for information from the system and on which individual **(383 DM 7.7 and 43 CFR 2.57)?**	
IV. Transfer of Privacy Act Records a. Are there procedures in place at the location that addresses the proper transfer of information from Privacy Act systems **(383 DM 8.7)?**	
b. When records are transferred to Federal Records Center or other facilities are 384 DM 4 followed?	
c. If information is moved, is it properly marked, and are handling instructions and use identified?	
V. Destruction of Privacy Act Records a. Does this system have a records schedule? If so, what is it?	
b. Are the records handled according to National Archives regulations at 36 CFR 1228.74. **(383 DM 8.8 and DOI Record's Management requirements)?**	

Attachment VII

FOR EXAMPLE PURPOSES ONLY

Rules of Behavior

Electronic Tracking FOIA System (EFTS)
Office of the Chief Information Officer (OCIO)
Department of the Interior (DOI)

The rules of behavior contained in this document are to be followed by all users of the EFTS. Users are expected to comply with this and all other DOI policies and will be held accountable for their actions while using the EFTS. Users must comply with the requirements of the Freedom of Information Act (FOIA) (5 U.S.C. 552), Privacy Act (PA) (5 U.S.C. 552a), Federal Records Act (44 U.S.C. Chapters 31 and 33), Federal Information Security Management Act, Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR Part 2635), and DOI's implementing regulations. The EFTS is covered by three DOI PA system of records notices: DOI-71, Electronic FOIA Tracking System and FOIA Case Files; DOI-69, FOIA Appeals; and DOI-57, Privacy Act Files (available at http://www.access.gpo.gov/su_docs/aces/1999_pa.html) An employee's failure to comply with the requirements of the Privacy Act could lead to civil or criminal penalties and questions regarding suitability of the individual for that position. If an employee violates these Rules of Behavior, he or she may be subject to disciplinary action at the discretion of DOI management. **Either the OCIO Departmental FOIA Officer, EFTS System Manager, EFTS ISSO, or the Desktop and Server Administration Division of the National Business Center (NBC) may revoke a person's system access for a specific period of time if an employee violates these Rules of Behavior** and may take disciplinary actions up to and including removal from the Federal service in conformance with the Department's Handbook for Discipline and Adverse Actions, DM 752 Handbook 1, March 29, 2006).

Under the PA system of records notice DOI-71, DOI FOIA Officers and Coordinators in headquarters and field offices are the system managers for the data input into and maintained on the EFTS for their respective organizations. As such, they are responsible for complying with the system manager requirements under the PA and the Federal Information Security Management Act. Please refer to the attached list of references for more information regarding the roles and responsibilities of system managers.

The EFTS application resides on a Windows 2003 server which is behind its own firewall separated from the other Departmental offices.

Connection to the Internet – The EFTS is accessed through the Internet and you are governed by the Department of the Interior (DOI) policies regarding Internet use. When you have completed the EFTS training and are requesting user access privileges, you must provide your Bureau FOIA Officer or their designated back-up with your static IP address for your workstation computer. You are only permitted to access the EFTS **while in your federal workplace**, and not from a telework sight or any other "off-site" location. You are not permitted to use a wireless connection to access the EFTS.

Protection of copyright licenses (software) – The EFTS was designed and licensed as a FOIA tracking system and portions may not be downloaded or used for other purposes. There will be audits conducted on this system.

Record Retention Requirements - Users must follow DOI's records management policies. Any documents or e-mail created may be considered Federal records that must be preserved by being printed and filed and may not be deleted from the system before being saved in the system's backup process.

Record Retention Requirements for Cobell v. Kempthorne litigation – Although no Individual INDIAN TRUST data will be entered and/or scanned into the system, you are reminded that if you receive a request for IITD, you must follow the records retention requirements for the Cobell v. Kempthorne litigation. Users must print and file, in accordance with applicable Court and Departmental directives, any documents they have or create and any electronic mail messages they send or receive, including attachments that relate to the Three Functional Areas of:

- American Indian trust reform, including the High-Level Implementation Plan or any of its subprojects:
- The Cobell v. Kempthorne litigation; or
- Administration of Individual Indian Money (IIM) accounts.

In addition, users must to the best of their abilities protect any files or data related to individual Indian trust data from unauthorized access.

Unique user name – Each person logging onto the system will have a unique user name.

Use of passwords - Users are to use passwords of a length specified by the EFTS system administrator. The user's password should consist of a mix of 8 characters--uppercase, lowercase, and a number or other character, e.g., Ap7ples# or 1Ap7ples.

For security purposes, users will need to change their passwords every 60 (sixty) days. The passwords must be at least 8 characters in length and can never be reused. This will be an automatic prompt from the system. This is an IT security requirement.

If an individual does not use the system within 60 days, forgets the password, or if the password is compromised, the user will need to obtain a new password immediately. The user must contact the Bureau FOIA Officer (or Backup User Administrator for the Bureau) to obtain a new password. Passwords will not be sent to users via email. The User Administrator (or Backup User Administrator) will contact the user by telephone or send it to the user in a sealed envelope through the mail.

System privileges - Users are given access to the EFTS based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

Individual accountability – **While using the EFTS, users will be held accountable for their actions. Employees must protect all sensitive information from disclosure to unauthorized individuals or groups. This includes but is not limited to the following: users must make an effort to ensure that computer monitors are located in such a way as to eliminate viewing by unauthorized persons; users must lock their workstations when away from the desk as a preventative measure to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information. If an employee adversely impacts the operation of the EFTS, OCIO/NBC may remove the employee's access without notice to ensure the operation and availability for the rest of DOI.**

Restoration of service - **The availability of the EFTS is a concern to all users, and we will do our best to ensure that the system is available at all times during normal working hours. However, Bureaus and Offices are responsible for ensuring that they are able to provide critical services in the event the system is unavailable in accordance with continuity of operation plans. In addition, users are asked to cooperate with system management staff during outages, so that service can be restored for all users in a timely manner.**

I acknowledge receipt of and have read the rules of behavior for the EFTS.

Signature of User	Date
Printed Name	Office
Supervisor's Printed Name	Supervisor's Signature

PLEASE NOTE: These rules are subject to change. Users will be notified of updates via e-mail.

March 30. 2007

Attachment