

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
- National Institute of Science and Technology (NIST) 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 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 Security Plan 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(e)	
c. Are system managers familiar with the Privacy Act disclosure and use restrictions for this grouping of information (43 CFR 2.56). 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)	
d. 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(e) 383 DM 3.11 383 DM 7: Disclosure Procedures 383 DM 8: Safeguarding 383 DM 9: Handling PA Records	
e. Was a Privacy Impact Assessment done for the automated system?	
f. Was it used to help identify the privacy concerns and handling requirements?	

Requirement and Guidance Cite	Compliant (Yes/No)
g. Do contractors manage, use or handle information from the Privacy Act system? <ol style="list-style-type: none"> 1. Do contracts have appropriate Federal Acquisition Regulation (FAR) and DOI Acquisition Regulation privacy clauses (see FAR 52.224-1 and 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? 	
h. 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, <i>Federal Register</i> notice)	
i. 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 what 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? 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?	