

CONTRACTOR REQUIREMENTS DOCUMENT

DOE O 206.1, DEPARTMENT OF ENERGY PRIVACY PROGRAM

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) site/facility management contractors whose contracts involve the design, development or operation of a Privacy Act System of Record. In addition, the Personally Identifiable Information (PII) requirements in this CRD apply to any site management contractor that handles PII.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's or subcontractor's compliance with the requirements.

1. GENERAL REQUIREMENTS.

- a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, and take appropriate actions to assist DOE in complying with Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives.
- b. Ensure that contractor employees are aware of their responsibility for—
  - (1) safeguarding Personally Identifiable Information (PII) and
  - (2) complying with the Privacy Act.

2. SPECIFIC REQUIREMENTS. The contractor must do the following:

- a. Ensure contractor employees are made aware of their roles and responsibilities for reporting suspected or confirmed incidents involving the breach of PII.
- b. Ensure contractor employees are cognizant of the following DOE Privacy Rules of Conduct. At a minimum, ensure contractor employees—
  - (1) are trained in their responsibilities regarding the safeguarding of PII;
  - (2) do not disclose any PII contained in any SOR except as authorized;
  - (3) report any known or suspected loss of control or unauthorized disclosure of PII;
  - (4) observe the requirements of DOE directives concerning marking and safeguarding sensitive

information, including, when applicable, DOE O 471.3, Protecting and Identifying Official Use Only Information;

- (5) collect only the minimum PII necessary for the proper performance of a documented agency function;
  - (6) do not place PII on shared drives, intranets or websites without permission of the System Owner; and
  - (7) challenge anyone who asks to see the PII for which they are responsible.
- c. Ensure that contractor employees complete the Annual Privacy Training and sign the completion certificate acknowledging their responsibility for maintaining and protecting Privacy Act information prior to being authorized access to all information systems.
  - d. Ensure contractor employees are cognizant of the fact that all personal information collected, maintained, used, or disseminated on behalf of the Agency must be maintained in a Privacy Act SOR.
  - e. Ensure that contractor employees recognize differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, contractors must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.
  - f. Ensure contractor employees are cognizant of the fact that non-compliance with the Privacy Act carries criminal and civil penalties.