OFFICE OF SECURITY
INFORMATION COLLECTION PACKAGE
OMB 1910-1800
Description of Collections
(Detail for Item 2 of the Supporting Statement)
April 30, 2009

1. Data Report on Spouse/Cohabitant

In accordance with Executive Order (E.O.) 12968, Access to Classified Information, and E.O. 10450, Security Requirements for Government Employment, DOE must request an investigation into an individual's character, associations and loyalty prior to granting access to DOE classified information. This requires that the individual provide information on not only himself or herself, but on his or her spouse or cohabitant with whom the individual has a spouse-like relationship or similar bond of affection. Individuals, both Federal and contractor employees, who marry or cohabitate subsequent to the granting of an access authorization, must, therefore, complete a collection of information known as the "Data Report on Spouse/Cohabitant," in order to provide required information including the spouse/cohabitant's name, social security number, date and place of birth, address and country of citizenship. DOE O 472.1C, Personnel Security Activities, contains the Departmental policy for this collection.

Nuclear Materials Inventory

2. Concise Note
3. Physical Inventory Listing
4. Nuclear Material Transaction Report
5. Material Balance Report
6. ADP Transcription Sheet

The Nuclear Materials Management and Safeguards System (NMMSS) is the United States Government's system of accountancy for nuclear materials which are owned and used by the U.S. Government, leased to or owned by private companies within the U.S., produced and owned in foreign countries under conditions that bring them into U.S. safeguards interest, and produced in the U.S. and leased or sold to foreign governments. The system is owned and sponsored by the U.S. Government [U.S. Department of Energy (DOE) and the Nuclear Regulatory Commission]. DOE implementing policy is contained in DOE O 474.1A, Control and Accountability of Nuclear Materials and DOE M 474.1-2A, Manual for Nuclear Materials Management and Safeguards System Reporting and Data Submission. The sources of data reported to the NMMSS are many and varied depending upon the legal requirements, safeguards restrictions, and financial interests related to each facet of the nuclear industry. Attributes such as ownership, reporting identification symbol, material type, and foreign obligations are the guidelines and criteria for reporting these activities to the NMMSS. The primary data subsystem is comprised of three elements containing the data reported by and generated for, facilities regarding inventories, transactions and material balances. The inventory data represents a facility's holdings of nuclear material at a specified point in time. The transaction data is concerned with physical transfers of nuclear materials between facilities, including detailed information on both the shipments and receipts. The material balance data is derived from and generated by the NMMSS on a monthly basis utilizing transaction data in conjunction with the

inventory data. Concise Notes are to accompany the submission of transaction, material balance and physical inventory data, as appropriate, for conveying explanatory information to the IAEA. The background data subsystem contains a variety of authority reference information which can be categorized as organizations, nuclear materials, projects, financial correlations, contracts, transportation, imports/exports/retransfers, foreign obligation information, and material balance categories.

7. Safeguards and Security Site Self Assessments
This collection of information is required by the National Industrial Security Program Operating Manual (NISPOM), which was established by E.O. 12829 "National Industrial Security Program." The NISPOM establishes the baseline requirements for the protection and control of classified information and is administered by the Information Security Oversight Office (ISOO) as part of the National Archives and Records Administration (NARA). This requirement is implemented by the Department through DOE O 470.4A, Safeguards and Security Program, DOE M 470.4-1, Safeguards and Security Program Planning and Management, and DOE M 470.4-4, Information Security. This collection is used to provide documentation on the quality of the security programs used by contractors to protect classified information, special nuclear material, and other national security assets. The report is prepared by the program office with oversight responsibilities for that specific site/contract. A similar report is prepared by the contractor. This report is called the safeguards and security site self assessment report.

8. Site Safeguards and Security Plans or Site Security Plans (for classified information)
This collection of information is required by the National Industrial Security Program Operating Manual (NISPOM), which was established by E.O. 12829 "National Industrial Security Program." The NISPOM establishes the baseline requirements for the protection and control of classified information and is administered by the Information Security Oversight Office (ISOO) as part of the National Archives and Records Administration (NARA). This requirement is implemented by the Department through DOE O 470.4A, Safeguards and Security Program, DOE M 470.4-1, Safeguards and Security Program Planning and Management, and DOE M 470.4-4, Information Security. This collection is used to provide documentation on the implementation measures used by contractors to protect classified information, special nuclear material, and other national security assets. These are prepared by the contractor and approved by the cognizant security office. These plans are updated as needed, or depending on the type of classified information / assets on at least an annual basis.

9. Site Safeguards and Security Plans or Site Security Plans (for unclassified information)
The Department does not have any collection of information identified as unclassified document security. The Department does have Site Safeguards and Security Plans and Site Security plans that identify the implementation of protection requirements for unclassified documents marked as containing Unclassified Controlled Nuclear Information and Official Use Only. The Departments requirement for these plans are contained in DOE O 470.4A, Safeguards and Security Program, DOE M 470.4-4, Information Security, DOE O 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information, DOE M 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information, DOE O 471.3, Identifying and Protecting Official Use Only Information, and DOE M 471.3-1, Manual for Identifying and Protecting Official Use Only Information. This collection is used to provide documentation on

the implementation measures used by contractors to protect unclassified information. These are prepared by the contractor and approved by the cognizant security office.

10. Foreign Ownership, Control, or Influence (FOCI)
The following is collected from bidders on DOE contracts requiring access authorizations (personnel security clearances). The information is required for DOE to (1) collect and analyze pertinent FOCI information, (2) validate reported FOCI information, and (3) adjudicate FOCI cases. This data must also be submitted by the bidder's tier parents, if any. The bidder and, if applicable, each tier parent must submit a completed SF-328, "Certificate Pertaining to Foreign Interests," a list of Key Management Personnel (KMP) to include its owners, officers, directors, and executive personnel that discloses the following for each: full name; all company titles/positions held; date and place of birth; social security number; and personnel security clearance, if any. The list must also provide the company's legal name, physical address of the facility location, and address of the company's principal executive offices, if different from the physical address.

11. Security Incident Notification and Preliminary Inquiry Report
This collection is used to document the events, facts, and circumstances surrounding security incidents. The Report of Security Incident/Infraction and Security Incident Notification are completed to document the facts and circumstances for security incidents. DOE M 470.4-1, Safeguards and Security Program Planning and Management, Part 2, Section N, Incidents of Security Concern, contains the Departmental policy for this collection.

12. Foreign Travel Management System (FTMS)
Transferred to MA-45 due to a reorganization. Removed from the Security package.

13. Foreign Access Central Tracking System
The Foreign Access Central Tracking System (FACTS) is the secure unclassified DOE national electronic tracking system that facilitates appropriate reviews, records approvals of visits and assignments by foreign nationals, and provides a historical database of biographical, visit and assignment, and approval information for the DOE complex. The system was created in response to Presidential Decision Directive 61, which recognized the need, at the executive level, to create a system to track foreign national visits and assignment information at Department of Energy sites. DOE O 142.3, Unclassified Foreign Visits and Assignments Program, contains the Departmental policy for this collection.

14. Vulnerability Assessments
Vulnerability Assessments are used by the Office of Security Technology and Assistance (HS-80) to support the analysis of deviations from Departmental and National security policy; analysis and support of budget data with respect to safeguards and security upgrade projects; analysis and validation of site security programs for system effectiveness and risk management decisions; validation and recommendations for implementing the Department's security design basis threat document; and to provide recommendations to sites and program offices on effective implementation of new technology and approaches to security. VA's are conducted as specified in DOE M 470.4-1, Safeguards and Security Program Planning and Management, Part 1, Section E, Vulnerability Assessment Program.

15. Request for Visitor Access Approval
In accordance with DOE M 470.4-1, Part 2, Section L, procedures to verify the visitor's identity, programmatic need-to-know, and that the visitor's clearance or access authorization is at least equal to the classification of the information to which access is being requested are in place. DOE F 56311.20 "Request for Visit or Access Approval" forms must be completed by Department of Energy (DOE) Federal and contractor employees to obtain programmatic approval for Sigma access. This form does not need to be submitted to visit Department facilities. A DOE security badge will serve as evidence of DOE access authorization. Other Government Agency (OGA) and OGA Contractor employees must also use this form or one similar in content to obtain access approval for visits to DOE facilities.

16. DOE Form 472.1 "Fair Credit Reporting Act Authorization"
In accordance with the Atomic Energy Act of 1954, as amended, Executive Order (E.O.) 12968, Access to Classified Information, and E.O. 10450, Security Requirements for Government Employment, DOE must request an investigation into an individual's character, associations and loyalty prior to granting access to DOE classified information. As deemed necessary by DOE, individuals may be required to provide credit information on themselves to DOE. Individuals, both Federal and contractor employees, complete an authorization known as the "Fair Credit Reporting Act Authorization," in order to allow DOE to collect such financial information. The form requests that the individual provide their name and social security number. DOE O 472.1C, "Personnel Security Activities," and any revisions thereto, contains the Departmental policy for this collection.

17. DOE Form 5631.5, "The Conduct of Personnel Security Interviews Under DOE Security Regulations"
In accordance with the Atomic Energy Act of 1954, as amended, Executive Order (E.O.) 12968, Access to Classified Information, and E.O. 10450, Security Requirements for Government Employment, DOE must conduct an interview into an individual's character, associations and loyalty, as deemed necessary, when determining eligibility for access to DOE classified information. This requires that the individual be advised of the process and of the ramifications of providing false or misleading information. Individuals, both Federal and contractor employees, complete a certification known as the "The Conduct of Personnel Security Interviews Under DOE Security Regulations," in order to ensure the individual's understanding of the interview process. DOE O 472.1C, "Personnel Security Activities," and any revisions thereto, contains the Departmental policy for this collection.

18. DOE Form 5631.18, "Security Acknowledgement"
In accordance with the Atomic Energy Act of 1954, as amended, Executive Order (E.O.) 12968, Access to Classified Information, and E.O. 10450, Security Requirements for Government Employment, DOE ensures that individuals are aware of the obligations associated with having access to Restricted Data and an understanding of what types of information that may raise a doubt as to their eligibility for DOE access authorization. Individuals, both Federal and contractor employees, complete a certification known as "Security Acknowledgement" in order to ensure their understanding of Restricted Data and other classified information, as well as their responsibilities associated with having access to such information. DOE O 472.1C, "Personnel

Security Activities," and any revisions thereto, contains the Departmental policy for this collection.

19. DOE Form 5631.29, "Security Termination Statement"
In accordance with the Atomic Energy Act of 1954, as amended, Executive Order (E.O.) 12968, Access to Classified Information, and E.O. 10450, Security Requirements for Government Employment, DOE ensures that individuals are aware of the obligations associated with the forthcoming termination of their access authorizations (security clearance) granted by DOE. Individuals, both Federal and contractor employees, complete a certification known as "Security Termination Statement" in order to ensure their understanding of their continued responsibility for protecting Restricted Data and other classified information to which they have gained knowledge while possessing a DOE access authorization. The form requests that the individual provide their name, social security number, date of birth, future residence, and future employer. DOE O 472.1C, "Personnel Security Activities," and any revisions thereto, contains the Departmental policy for this collection.